Утвержден

ВЕМР.00119-01-/1У

ПС «Купол-СКЗИ для Windows»

Инструкция по загрузке и настройке

ВЕМР.00119-01 99 01

Листов 19

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

2019

Литера $О_1$

АННОТАЦИЯ

Настоящий документ содержит сведения о назначении, функциях и структуре программного средства «Купол-СКЗИ для Windows» ВЕМР.00119-01 (далее по тексту – ПС «Купол-СКЗИ для Windows»). Описаны условия его выполнения, приведены сведения по установке и настройке, описаны процедуры запуска, завершения.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ СРЕДСТВЕ

1.1. Назначение программного средства

1.1.1. ПС «Купол-СКЗИ для Windows» предназначено для построения защищённых распределённых хранилищ данных.

1.2. Условия выполнения программного средства

1.2.1. ПС «Купол-СКЗИ для Windows» функционирует на ПЭВМ с характеристиками не ниже следующих:

- процессор Intel Core 2 Duo 1,8 ГГц;
- оперативная память 2048 Мбайт;
- жесткий диск 100 Гбайт;
- сетевая плата Fast Ethernet 100 Мбит/с.

1.2.2. Программное средство функционирует в среде ОС Microsoft Windows со встроенными и дополнительными интегрируемыми механизмами обеспечения безопасности, реализуемыми средством защиты информации «Secure Pack Rus версия 3.0 (исполнение 6)».

Защита информации на съемных носителях, обеспечивается с помощью "Secure Pack Rus" Версия 3.0 (SPR) подсистемой "Расширенные политики Шифрующей Файловой Системы (Enhanced Encrypting File System (EFS) Policies)" (далее - EFP), которая осуществляет мандатное управления атрибутами шифрования файлов (далее - мандатное шифрование) на съемных носителях информации. Использование мандатного шифрования обеспечивает возможность реализовать криптографическую изоляцию информации в корпоративной сети. См. документацию "Средство защиты информации «Secure Pack Rus» Версия 3.0 Мандатное шифрование".

С использованием EFS всем отчуждаемым носителям, находящимся в эксплуатации, должны быть присвоены мандатные метки, соответствующие грифу

обрабатываемой информации. Все отчуждаемые носители должны быть учтены режимно-секретным отделом организации, эксплуатирующей автоматизированную систему. Использование неучтенных отчуждаемых носителей должно быть запрещено.

2. УСТАНОВКА И НАСТРОЙКА ПРОГРАММНОГО СРЕДСТВА

2.1. Установка программного средства

При установке программного средства должны быть выполнены пункты раздела "Требования к установке и эксплуатации" документа "SPR 3.0 - Описание применения".

На всех дисках АРМ должна быть установлена файловая система NTFS.

Все используемые съемные устройств хранения должны быть предварительно отформатированы с использованием файловой системы NTFS.

2.1.1. Для установки комплекса программ необходимо:

– выполнить установку ОС Windows 10;

– скопировать каталог kupolcore/bin, находящийся на компакт–диске ВЕМР.00119-02 12 02 Исполняемые файлы на локальную машину в каталог C:\Kupol. В данном каталоге расположены бинарные файлы модулей и конфигурационные файлы (operator - файл, содержащий цифровые данные оператора РР, rrwserv.cfg - конфигурационный файл сервера, содержит имена директорий и команды вызовов модулей areestr и creestr, stopserv - файл, необходимый для остановки сервера РР).

2.1.2. Установка комплекса программ заключается в установке модулей программного средства:

– Пользовательский интерфейс;

– Модуль формирования сетевого имени (initus);

– Модуль генерации контейнеров для связи с оператором РР (gencrtk);

– Модуль изменения пароля (chpin);

– Модуль формирования файла для передачи оператору РР (rsen);

– Модуль проверки и экстракции файла (rrec);

– Модуль записи в РР (areestr);

– Модуль извлечения информации из РР по номеру звена (creestr);

– Модуль сервера PP (rrwserv).

2.2. Установка SPR 3.0

Программное обеспечение и эксплуатационная документация SPR 3.0 находится на установочном компакт-диске.

2.2.1. Установка полной версии SPR 3.0 необходимо запустить файл из дистрибутива соответствующий целевой программной платформе (x86 или x64). После запуска мастера установки, последовательно появляется серия окно установки (приветствия, лицензионного соглашения, выбора папки установки, подтверждения установки, прогресса инсталляции, завершения инсталляции). По окончании установки, чтобы изменения вступи в силу, необходима перезагрузка компьютера.

2.2.2. Установка оснасток настройки SPR 3.0

Для установки оснасток настройки SPR3.0, необходимо с установочного диска запустить файл spr-win32-snapins-rus.msi (spr-x64-snapins-rus.msi). И далее следовать указаниям установщика (аналогично предыдущему пункту).

2.3. Вывод графических окон сервисом КриптоПро CSP КС3

В процессе работы сервис CSP КриптоПро может выводить графические окна для взаимодействия с пользователем: информацию о ключевых носителях, приглашение на генерацию последовательностей случайных чисел для формирования ключевого материала и т.д.

Для корректного отображения окон информации сервисом CSP КриптоПро в ОС должны быть активированы необходимые компоненты, которые реализуют вывод информации с уровня сервиса на уровень пользователя.

Настройку корректного отображения окон информации сервисом CSP см. в документе "Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности." параграф "Настройка серверных ОС Windows Server 2008 / 2012"

2.3.1. Работа с окнами сервиса КриптоПро CSP КС3

При работе пользователя сервис CSP КриптоПро может выводить сообщения для взаимодействия с пользователем – пример такого сообщения представлен на рис. 1.

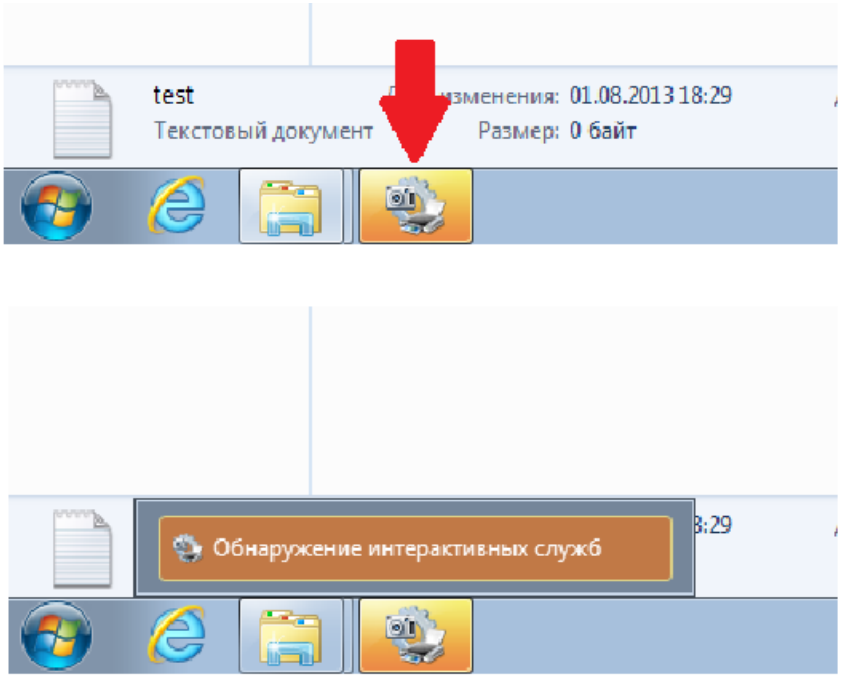

Рисунок 1

Возникновение такого сообщения означает, что криптографической подсистеме необходимо взаимодействие с пользователем.

Описание взаимодействия криптографической подсистемы с пользователем см. в документе "Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности." параграф "Работа с окнами сервиса КриптоПро CSP"

Взаимодействие с сервисом CSP КриптоПро можно отложить, не переходя в окно приглашения. Тем не менее, если пользователь перешел в окно приглашения, но выбрал действие «Спросить позже», запрос сервиса CSP КриптоПро будет завершен с ошибкой. Для повторного взаимодействия с сервисом CSP КриптоПро может потребоваться перезагрузка АРМ.

2.4. Политики защиты критических ресурсов

2.4.1. Идентификация пользователей

Подсистема доверенной аутентификации должна базироваться на подсистеме идентификации и аутентификации ОС Microsoft Windows и дополнятся продуктом компании КриптоПро Winlogon. Аутентификация пользователя производится путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов.

Настройки политики паролей осуществляется в оснастке "Управление групповой политикой".

Для внесения изменения в политику паролей, необходимо запустить оснастку "Управление групповой политикой", найти DefaultDomainPolicy, нажать на ней правой кнопкой мыши и выбрать "Изменить"

Минимальные требования к качеству аутентификации:

Политика	**Краткое пояснение**	**Допустимые значения**
Вести журнал паролей/ Enforce password history	Определяет число новых уникальных паролей	4
Максимальный срок действия пароля/ Maximum password age	Определяет период времени (в днях), в течении которого можно использовать пароль, пока система не потребует сменить его.	90
Минимальная длина пароля / Minimum password lenght	Параметр определяет минимальное количество знаков, которое должно содержаться в пароле	8
Минимальный срок действия пароля/ Minimum password	Параметр определяет период времени (в днях) в течении	0

age	которого пользователь должен использовать пароль, прежде чем его можно будет изменить.	
Пароль должен отвечать требованиям сложности / Password must meet complexity requirements	Параметр определяет должен ли пароль отвечать сложности: -не содержать имени учетной записи - длина не менее 8 знаков - содержать заглавные буквы (F, G,R) - содержать строчные буквы (f,y,x) - содержать цифры	Вкл.
Хранить пароли, используя обратимое шифрование / Store password susing reversible encryption	Параметр указывает использовать ли операционной системой для хранения паролей обратимое шифрование.	Вкл.

Для внесения изменения в требования к установке паролей необходимо запустить "Конфигурация компьютера"- "Политики"- "Конфигурация Windows"- "Параметры безопасности"- "Политики учетных записей"- “Политика блокировки учетной записи”. в правом окне расположены параметры пароля, которые применяются в домене.

Минимальные требования к настройкам блокировок:

Политика	**Краткое пояснение**	**Допустимые значения**
Время до сброса счетчика блокировки	Определяет количество минут, которые должны истечь после неудачной попытки входа в систему, до того как счетчик	30 мин

	неудачных попыток входа будет сброшен до 0	
Пороговое значение блокировки	Определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет сброшена администратором, либо пока не истечет период блокировки этой учетной записи.	6
Продолжительность блокировки учетной записи	Определяет количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки	30 мин

2.4.2. Регистрация событий

Регистрация событий осуществляется путём автоматизированного ведение журнала событий, связанных с работой системы, посредством системы «Secure Pack Rus» версия 3.0.

Сведения, необходимые для настройки и управления журналами см. в документе "Руководство администратора безопасности. Аудит. Средство защиты информации «Secure Pack Rus» версия 3.0."

В журнале подлежат регистрации следующие события:

- Создание новой, модификация (удаление) существующей учетной записи пользователя.
- Изменение прав пользователя
- Вход / выход пользователей в систему
- расчет контрольных сумм защищаемых файлов.

- проверки контрольных сумм защищаемых файлов.
- попытка получения доступа к защищаемому объекту.
- попытка получения доступа к объекту файловой системы на контролируемом съемном носителе.

Контролю подлежат следующие исполняемые модули:

initus.exe; gencrtk.exe; chpin.exe; rsen.exe; rrec.exe; areestr.exe; creestr.exe; rrwserv.exe, а также конфигурационный файл rrwserv.cfg.

Записи аудита доступа к объекту должны включать не только сам факт разрешенного или запрещенного доступа, но также и причину успеха или отказа. Описание работы подсистемы аудита безопасности сценариев SPR 3.0 представлено в документе "Руководство администратора безопасности. Аудит. Средство защиты информации «Secure Pack Rus» версия 3.0."

2.4.3. Защита объектов файловой системы

При формировании политики защиты объектов файловой системы необходимо добавить в список для контроля следующие пути ФС:

- C:\Windows;
- C:\Program Files;
- C:\Program Files (x86) (При использовании 64-разрядных ОС).

Данные правила обеспечат контроль целостности объектов ФС в составе ОС и ОПО при установке ОС по умолчанию (на системный диск «С»). При установке ОС/ОПО/СПО по нестандартным путям, следует выполнить соответствующую модификацию указанных путей ФС.

После первоначальной установки SPR 3.0 политика защиты объектов файловой системы включена в режиме Аудит. Контроль доступа пользователей к критическим объектам файловой системы не производится!

При первоначальной установке SPR3.0 список правил доступа к съемным носителям пуст, поэтому активация политики приведет к полной блокировке всех классов съемных носителей. После установки SPR3.0 и создания базового набора

правил доступа необходимо включить контроль за подключением съемных носителей.

При первоначальной установке SPR3.0 список правил защиты объектов файловой системы пуст, поэтому активация политики не приводит к блокировке модификации каких-либо областей файловой системы.

Для изменения режима работы политики необходимо:

• раскрыть в консоли управления политиками следующий путь: Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Защита критических ресурсов→Файловая система и, вызвав меню, выбрать радел «Свойства» и в открывшемся окне отметить пункт «Активировать действие правил» (рис.2).

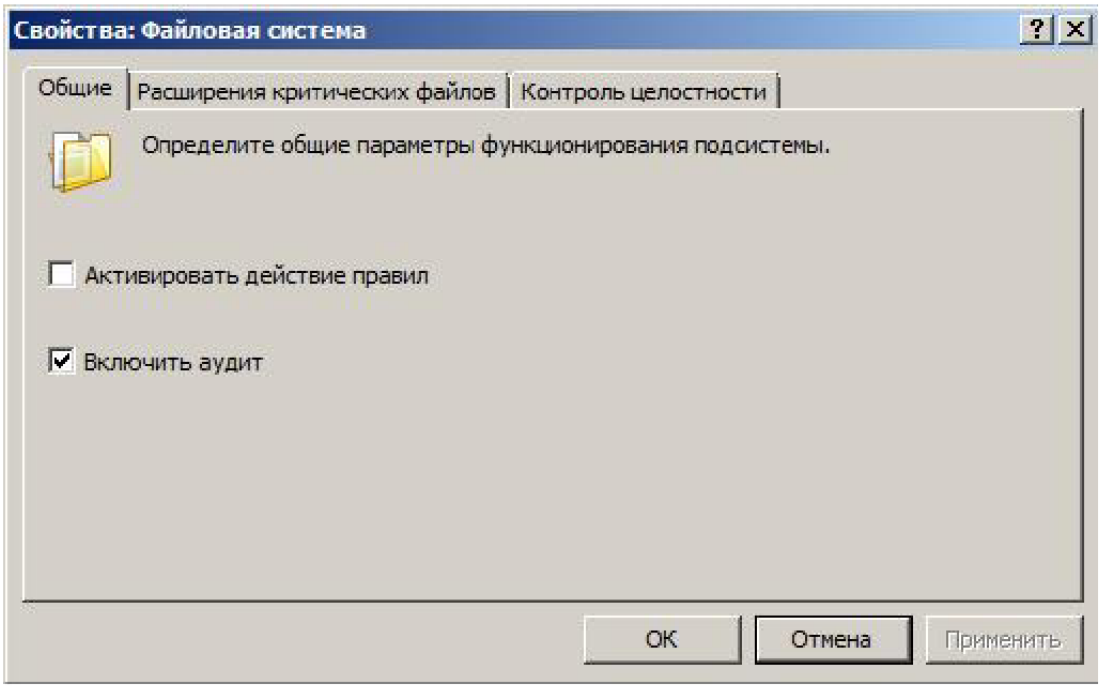

Рисунок 2

Для изменения набора расширений критических файлов необходимо раскрыть в консоли управления политиками следующий путь: Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Защита критических ресурсов→Файловая система и, вызвав меню, выбрать радел «Свойства», в открывшемся выбрать закладку «Расширения критических файлов» (рис. 3)

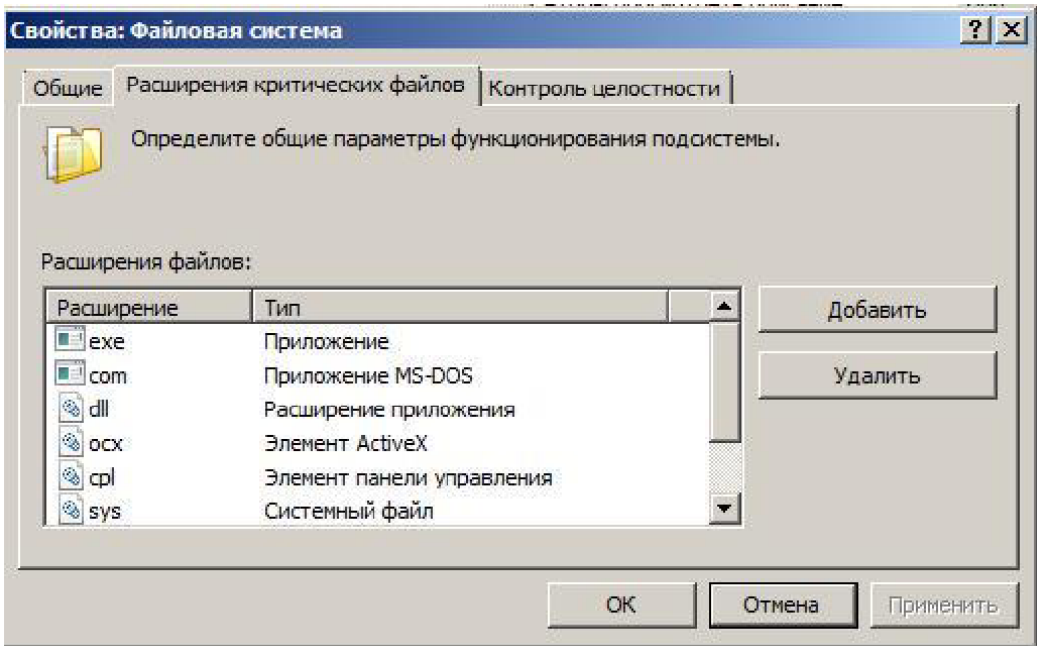

Рисунок 3

2.5. Контроль целостности критических файлов

Контролю целостности подлежат следующие исполняемые модули:

initus.exe; gencrtk.exe; chpin.exe; rsen.exe; rrec.exe; areestr.exe; creestr.exe; rrwserv.exe, а также конфигурационные файлы rrwserv.cfg, operator, stopserv.

Контроль целостности реализуется в соответствии ГОСТ Р 34.11-94 путём:

- расчета контрольных сумм файлов
- проверки контрольных сумм файлов
- защиты от модификаций файлов, для которых, в соответствии с установленной политикой, проверяются контрольные суммы.

Для контроля целостности используется подсистема защиты критических ресурсов SPR 3.0. Которая осуществляет слежение за неизменностью контролируемых объектов файловой системы. Она также обеспечивает запрета на модификацию объектов ФС, стоящих на контроле.

Контроль должен проводится в автоматическом режиме не реже 1 раз в сутки с момента загрузки ОС.

Описание работы подсистемы защиты критических ресурсов SPR 3.0 представлено в документе "Руководство администратора безопасности." Средство защиты информации «Secure Pack Rus» версия 3.0.

2.5.1. Политика управления приложениями (AppLocker)

Политика управления приложениями позволяет администраторам ограничивать запуск пользователями нежелательных или ненадежных приложений на серверах и рабочих станциях, работающих как в сценарии домена, так и в рабочей группе.

Для применения политик управления приложениями (AppLocker) на АРМ необходимо наличие лицензии ОС уровня «Корпоративная» или «Максимальная». На АРМ с лицензией ОС уровня «Профессиональная» следует использовать политики ограниченного использования программ (SRP).

2.5.2. Требования к базовым настройкам

Базовые настройки политики управления приложениями должны включать следующие ограничения запуска:

- Исполняемые файлы

1. Path - %PROGRAMFILES%* - everyone
2. Path - %WINDIR%* - everyone
3. Path - * - Administrators

- Установщики

1. Publisher - Signed – everyone
2. Path - %WINDIR%\Installer* - everyone
3. Path - * - Administrators

- Запуск скриптов

1. Path - %PROGRAMFILES%* - everyone
2. Path - %WINDIR%* - everyone
3. Path - * - Administrators

В дополнение к базовым настройкам, необходимо запретить для всех групп пользователей кроме Администраторов запуск следующих программ: %WINDIR%\system32\regsvr32.exe, %WINDIR%\system32\rundll32.exe, %WINDIR%\system32\subst.exe, %WINDIR%\system32\mklink.exe.

2.6. Удаление комплекса программ

2.6.1. Для удаления комплекса программ необходимо выполнить следующие действия:

– удалить директорию C:\Kupol;

2.7. Настройка комплекса программ

2.7.1. Дополнительных действий по настройке комплекса программ выполнять не требуется.

3. ЗАПУСК И ЗАВЕРШЕНИЕ КОМПЛЕКСА ПРОГРАММ

3.1. Запуск и завершение

3.1.1. Запуск программы осуществляется с помощью двойного нажатия левой клавиши «мыши» на ярлыке «Купол-СКЗИ», расположенном на рабочем столе операционной системы (рис. 1).

Ярлык «Купол-СКЗИ»

Рис. 1

3.1.2. Завершение работы программы происходит при нажатии левой клавиши «мыши» на кнопке «X» главного окна программы «Пользовательский интерфейс». Необходимо подтвердить свои действия (рис.2).

Выход из программы

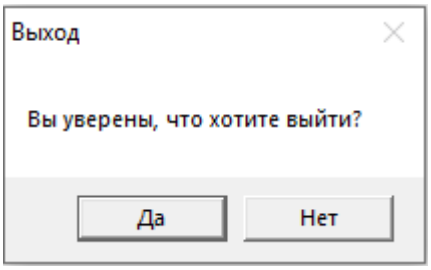

Рис. 2

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

РР	–	распределенный реестр
ПС	–	программное средство
ОС	–	операционная система
ПЭВМ	–	персональная электронная вычислительная машина
СН	–	специального назначения

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					