Средство защиты информации

«Secure Pack Rus»

Версия 3.0

Описание применения

EAPM.5090005.032-03 31 01

Листов 18

Компания «СиЭйЭн»

2016

Компания «СиЭйЭн»
Адрес 107140, г. Москва, Московско-Казанский пер., д. 11-15
Телефон +7 (495) 666-5606
e-mail info@cansec.ru
Web www.cansec.ru

Оглавление

Список сокращений

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ЗПС	Замкнутая программная среда
ИС	Информационная система
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СЗИ	Средство или система защиты информации
СКЗИ	Средство криптографической защиты информации
СХКИ	Средство хранения конфиденциальной информации

1. Назначение программы

Средство защиты информации «Secure Pack Rus» версия 3.0 (сокращенные названия изделия – Secure Pack Rus 3.0 или SPR 3.0) предназначено для обеспечения защиты информационных ресурсов АИС, состоящих из АРМ и серверов, функционирующих под управлением ОС компании Microsoft (Таб. 1, Таб. 2 и Таб. 3), и совместно с другими средствами защиты усиливает штатные механизмы ОС, обеспечивающие информационную безопасность АИС.

Таб. 1. Операционные системы, поддерживаемые SPR 3.0 (Исполнения 1, 2)

Операционная система	Пакет обновления	Необходимые дополнительные обновления
Microsoft Windows XP Professional[1]	Service Pack 3	
Microsoft Windows Server 2003 R2 Standard/Enterprise Edition[1]	Service Pack 2	
Microsoft Windows Server 2003 R2 Standard/Enterprise x64 Edition[1]	Service Pack 2	
Microsoft Windows 7 Professional/Enterprise/Ultimate[1]	Service Pack 1	
Microsoft Windows 7 Professional/Enterprise/Ultimate x64 Edition[1]	Service Pack 1	
Microsoft Windows Server 2008 R2 Standard/Enterprise[1]	Service Pack 1	

Примечания: [1] Порядок и сроки эксплуатации ОС определяются производителем ОС.

Таб. 2. Операционные системы, поддерживаемые SPR 3.0 (Исполнения 3, 4)

Операционная система	Пакет обновления	Необходимые дополнительные обновления
Microsoft Windows 7 Professional/Enterprise/Ultimate[1]	Service Pack 1	
Microsoft Windows 7 Professional/Enterprise/Ultimate x64 Edition[1]	Service Pack 1	

Microsoft Windows Server 2008 R2 Standard/Enterprise[1]	Service Pack 1
Microsoft Windows 8 Pro/Enterprise[1]	
Microsoft Windows 8 Pro/Enterprise x64 Edition[1]	
Microsoft Windows Server 2012 Standard[1]	
Microsoft Windows 8.1 Pro/Enterprise[1]	
Microsoft Windows 8.1 Pro/Enterprise x64 Edition[1]	
Microsoft Windows Server 2012 R2 Standard[1]	

Примечания: [1] Порядок и сроки эксплуатации ОС определяются производителем ОС.

Таб. 3. Операционные системы, поддерживаемые SPR 3.0 (Исполнения 5, 6)

Операционная система	Пакет обновления	Необходимые дополнительные обновления
Microsoft Windows 7 Professional/Enterprise/Ultimate[1]	Service Pack 1	KB3033929
Microsoft Windows 7 Professional/Enterprise/Ultimate x64 Edition[1]	Service Pack 1	KB3033929
Microsoft Windows Server 2008 R2 Standard/Enterprise[1]	Service Pack 1	KB3033929
Microsoft Windows 8 Pro/Enterprise[1]		
Microsoft Windows 8 Pro/Enterprise x64 Edition[1]		
Microsoft Windows Server 2012		

Standard[1]	
Microsoft Windows 8.1 Pro/Enterprise[1]	
Microsoft Windows 8.1 Pro/Enterprise x64 Edition[1]	
Microsoft Windows Server 2012 R2 Standard[1]	
Microsoft Windows 10 Pro/Enterprise x64 Edition[1]	Windows 10 Version 1511 (build 10.0.10586)
Microsoft Windows 10 Pro/Enterprise Edition[1]	Windows 10 Version 1511 (build 10.0.10586)

Примечания: [1] Порядок и сроки эксплуатации ОС определяются производителем ОС.

SPR 3.0 поставляется в четырех исполнениях.

ОС Microsoft Windows (Таб. 1, Таб. 2) со встроенными и дополнительными интегрированными механизмами обеспечения безопасности, реализуемыми SPR 3.0 Исполнение 1 и SPR 3.0 Исполнение 3, обеспечивает уровень защиты АК3 в соответствии с (1) и реализует:

- Возможность доменной аутентификации пользователей на основе метода двухфакторной аутентификации с использованием сертификатов стандарта X.509.
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к именованным объектам системы (файлы, процессы и т.д.).
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к устройствам (отчуждаемые хранилища данных, мобильные устройства, принтеры, порты ввода/вывода и т.д.).
- Обнуление освобожденной оперативной памяти системы.
- Возможность аудита входа/выхода субъектов доступа (пользователей) в систему/из системы.
- Возможность аудита.
- Возможность периодического контроля целостности объектов файловой системы.
- Возможность задания администратором списка разрешенных на выполнение программных модулей.
- Возможность задания администратором списка разрешенных для установки в систему инсталляционных пакетов.
- Возможность задания администратором списка разрешенных на выполнение сценариев.
- Возможность криптографической защиты информации, передаваемой по канал связи, с посредством создания аутентичного защищенного соединения с использованием протокола КриптоПро TLS и/или посредством защиты IP-соединений с использованием протоколов КриптоПро IKE, КриптоПро ESP, КриптоПро AH. Криптографическая защита информации осуществляется по классу КС3.
- Возможность криптографической защиты информации, записываемой на съемные хранилища данных посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС3.
- Возможность криптографической защиты информации, записываемой на жестких дисках АРМ и серверов посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС3.
- Возможность централизованного удаленного управления через механизм групповых политик ОС Microsoft Windows (Таб. 1, Таб. 2).

ОС Microsoft Windows (Таб. 1, Таб. 2) со встроенными и дополнительными интегрированными механизмами обеспечения безопасности, реализуемыми SPR 3.0

Исполнение 2 и SPR 3.0 Исполнение 4, обеспечивает уровень защиты АК2 в соответствии с (1) и реализует:

- Возможность доменной аутентификации пользователей на основе метода двухфакторной аутентификации с использованием сертификатов стандарта X.509.
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к именованным объектам системы (файлы, процессы и т.д.).
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к устройствам (отчуждаемые хранилища данных, мобильные устройства, принтеры, порты ввода/вывода и т.д.).
- Обнуление освобожденной оперативной памяти системы.
- Возможность аудита входа/выхода субъектов доступа (пользователей) в систему/из системы.
- Возможность аудита.
- Возможность периодического контроля целостности объектов файловой системы.
- Возможность задания администратором списка разрешенных на выполнение программных модулей.
- Возможность задания администратором списка разрешенных для установки в систему инсталляционных пакетов.
- Возможность задания администратором списка разрешенных на выполнение сценариев.
- Возможность криптографической защиты информации, передаваемой по канал связи, с посредством создания аутентичного защищенного соединения с использованием протокола КриптоПро TLS и/или посредством защиты IP-соединений с использованием протоколов КриптоПро IKE, КриптоПро ESP, КриптоПро AH. Криптографическая защита информации осуществляется по классу КС2.
- Возможность криптографической защиты информации, записываемой на съемные хранилища данных посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС2.
- Возможность криптографической защиты информации, записываемой на жестких дисках АРМ и серверов посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС2.
- Возможность централизованного удаленного управления через механизм групповых политик ОС Microsoft Windows (Таб. 1, Таб. 2).

2. Условия применения

SPR 3.0 эксплуатируется в составе АИС, состоящих из АРМ и серверов, функционирующих под управлением ОС компании Microsoft (Таб. 1, Таб. 2).

2.1. Требования к аппаратным средствам

Требования к аппаратным средствам приведены в таблицах Таб. 4-Таб. 9.

Таб. 4. Системные требования для ОС Microsoft Windows XP Professional

Компонент	Требование
Компьютер и процессор	Процессор с частотой не менее 233 МГц или более быстрый (рекомендуется не менее 300 МГц)
Память	Не менее 64 МБ оперативной памяти (рекомендуется не менее 128 МБ)
Жесткий диск	Не менее 1,5 ГБ свободного места на жестком диске

Таб. 5. Системные требования для ОС Microsoft Windows Server 2003 R2

Компонент	Требование
Компьютер и процессор	**Standard Edition** Компьютер с процессором с частотой не менее 133 МГц; рекомендуется 550 МГц или больше; поддержка до четырех процессоров на одном сервере **Enterprise Edition** Процессор с частотой не менее 133 МГц; рекомендуется 550 МГц; на одном сервере поддерживаются до восьми процессоров
Память	**Standard Edition** Не менее 128 МБ; рекомендуется 256 МБ и более; максимально 4 ГБ **Enterprise Edition** Не менее 128 МБ; рекомендуется 256 МБ и более; максимально 64 ГБ для компьютеров на базе x86; максимально 2 ТБ для компьютеров на базе x64
Жесткий диск	**Standard Edition** 1,2 ГБ для сетевой установки; 2,9 ГБ для установки с компакт-диска **Enterprise Edition** 1,2 ГБ для сетевой установки; 2,9 ГБ для установки с компакт-диска

Таб. 6. Системные требования для ОС Microsoft Windows 7

Компонент	Требование
Компьютер и процессор	32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 гигагерц (ГГц) или выше
Память	1 гигабайт (ГБ) (для 32-разрядной системы) или 2 ГБ (для 64-разрядной системы)
Жесткий диск	16 гигабайт (ГБ) (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) пространства на жестком диске

Таб. 7. Системные требования для ОС Microsoft Windows Server 2008 R2

Компонент	Требование
Компьютер и процессор	1,4 ГГц (процессор с архитектурой x64).
Память	Минимальный объем: 512 МБ. Максимальный объем: Standard Edition — 32 ГБ, Enterprise Edition — 2 ТБ.
Жесткий диск	Минимальный объем: 32 ГБ. Примечание. На компьютерах, оснащенных более чем 16 ГБ ОЗУ, потребуется больше места на диске для файлов подкачки, спящего режима и дампа памяти.

Таб. 8. Системные требования для ОС Microsoft Windows 8/8.1/10

Компонент	Требование
Компьютер и процессор	32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 гигагерц (ГГц) или выше с поддержкой PAE, NX и SSE2
Память	1 гигабайт (ГБ) (для 32-разрядной системы) или 2 ГБ (для 64-разрядной системы)
Жесткий диск	16 гигабайт (ГБ) (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) пространства на жестком диске
Графическая карта	Microsoft DirectX 9 с драйвером WDDM

Таб. 9. Системные требования для ОС Microsoft Windows Server 2012/2012 R2

Компонент	Требование

Компьютер и процессор	1,4 ГГц (процессор с архитектурой x64).
Память	Минимальный объем: 512 МБ.
Жесткий диск	Минимальный объем: 32 ГБ.

2.2. Требования к установке и эксплуатации

Для обеспечения защиты информации при эксплуатации SPR 3.0 необходимо соблюдение следующих общих условий применения:

- Установка и настройка SPR 3.0 должна производиться в соответствии с (2), (3), (4), (5) и (6).
- Должна быть обеспечена (организационно-техническими мерами) невозможность бесконтрольного доступа к отчуждаемым носителям и кабельной системе со стороны незарегистрированных пользователей АИС.
- Выставляемые при инсталляции настройки системных привилегий и дискреционных прав доступа к объектам файловой системы и ключам реестра не должны расширяться в ходе эксплуатации АИС.
- В ходе эксплуатации АИС не должны подвергаться модификации ключи реестра, используемые SPR 3.0 для управления.
- Учетная запись «Гость» должна быть отключена.
- Для обнуления файла подкачки страниц должна быть активирована политика «Очистка файла подкачки страниц памяти».
- В случае аварийного завершения работы (например, выключения электропитания) необходимо произвести запуск системы с последующим завершением работы стандартными средствами.
- Размер системных журналов протоколирования не должен быть менее 512 килобайт.
- На всех дисках АРМ должна быть установлена файловая система NTFS.
- На всех АРМ должны быть заблокированы порты IEEE 1394 (Firewire).
- СКЗИ, входящее в состав SPR 3.0, может использоваться ППО для реализации криптографической защиты обрабатываемых и передаваемых данных при условии обеспечения корректности взаимодействия с СКЗИ и реализации мер по обеспечению безопасности ключевой системы.
- Разработка и использование ППО должна производиться в соответствии с рекомендациями разработчика СКЗИ. В случае использования ППО для криптографической защиты обрабатываемых данных в АИС государственных информационных ресурсов необходимо проведение сертификационных испытаний указанного ППО установленным порядком.

- Программы, образующие доверенную программную среду, не должны содержать в себе средств разработки или интерпретаторов, а также скрытых и/или явных возможностей, позволяющих нарушить штатное функционирование механизмов программных СЗИ и/или создавать каналы утечки информации, в частности:
  - модифицировать собственный код и код общих модулей, спроецированных в оперативную память процесса;
  - просматривать и модифицировать память, выделенную для других процессов; для драйверов, кроме того, просматривать и модифицировать память, выделенную для других драйверов;
  - передавать управление в область собственных данных и данных других процессов;
  - выполнять просмотр и редактирование файлов в обход стандартных функций ОС для работы с файлами, а также жестких дисков на уровне секторов;
  - открывать непосредственный доступ к портам ввода/вывода для программ прикладного уровня.

Должна быть обеспечена физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации.

3. Описание задачи

Интеграция механизмов обеспечения безопасности SPR 3.0 в ОС Microsoft Windows (Таб. 1, Таб. 2) и их использование совместно с базовыми механизмами позволяет обеспечить общий уровень защиты ОС до АК3 в соответствии с (1).

SPR 3.0 интегрируется в ОС Microsoft Windows (Таб. 1, Таб. 2) как ее часть и базируется на документированных механизмах защиты информации ОС, что обеспечивает высокую устойчивость работы и совместимость с другими программными продуктами.

3.1. Подсистемы SPR 3.0

SPR 3.0 состоит из четырех подсистем:

- Подсистема управления политиками
- Подсистема защиты критических ресурсов
- Подсистема контроля доступа к устройствам
- Подсистема мандатного шифрования
- Подсистема контроля запуска сценариев

3.2. Схема управления подсистемами

Общая схема управления подсистемами SPR 3.0 приведена на Рис. 1.

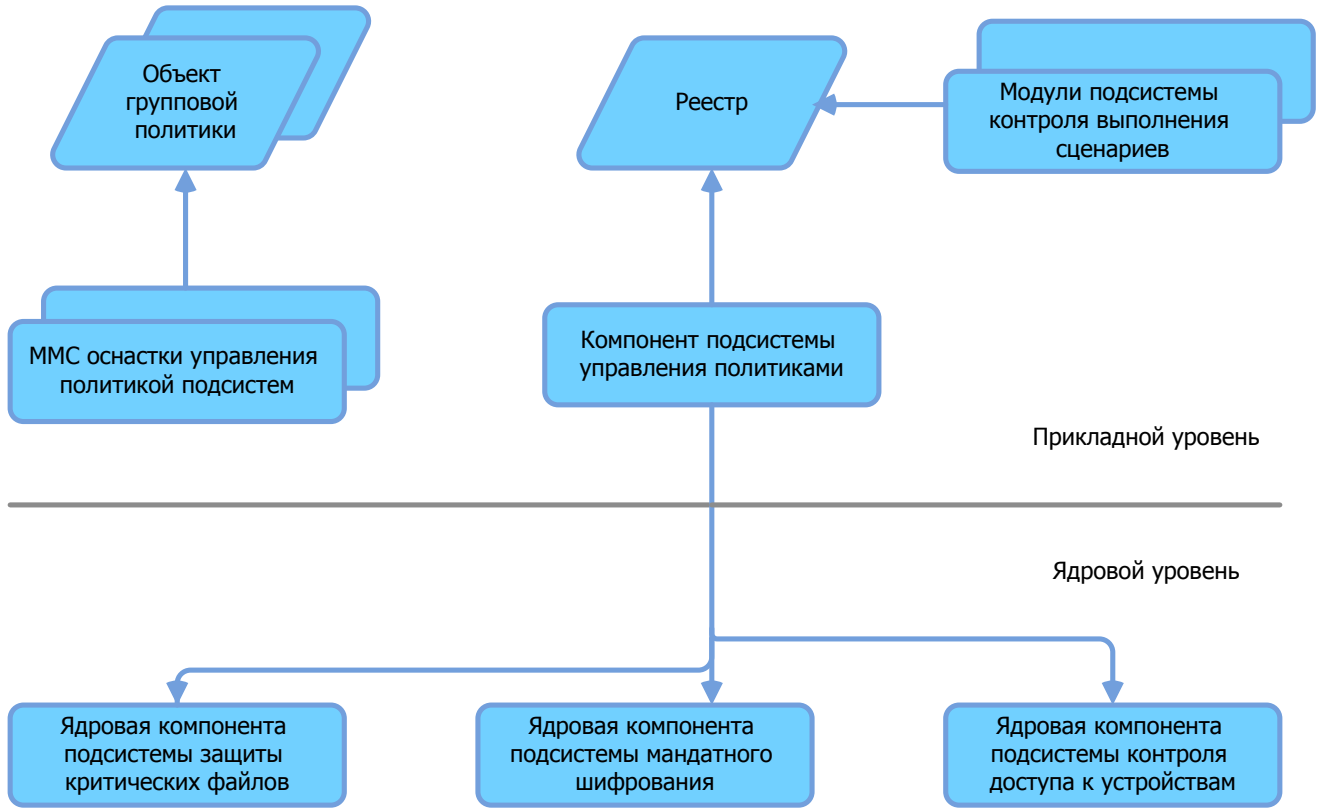
Управления политиками SPR 3.0 осуществляется посредством MMC оснасток интегрированных в системную оснастку «Параметры безопасности». Это позволяет администратору безопасности управлять всеми политиками безопасности, включая политики SPR 3.0, из одной консоли.

Параметры, установленные администратором безопасности в оснастках SPR 3.0, сохраняются в объектах групповой политики, откуда посредством механизма распространения групповых политик Windows они попадают в реестр.

Компонент подсистемы управления политиками считывает записанные в реестр настройки, форматирует их и передает ядровым компонентам соответствующих подсистем.

Данная схема управления позволяет не перегружать ОС при изменении политик SPR 3.0

Рис. 1 Общая схема управления подсистемами SPR 3.0



3.3. Подсистема защиты критических ресурсов

Подсистема защиты критических ресурсов SPR 3.0 реализует контроль целостности объектов файловой системы.

Контроль целостности реализуется на основе расчета функции хеша (контрольной суммы) файла по ГОСТ Р 34.11-94 с использованием ядровой компоненты СКЗИ КриптоПро CSP.

Подсистема состоит из ММС оснастки управления и ядровой компоненты.

Ядровая компонента подсистема защиты критических ресурсов реализует три основные функции:

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

3.4. Подсистема контроля доступа к устройствам

Подсистема контроля доступа к устройствам реализует функции разграничения доступа пользователей к различным устройствам (съемные диски, CD-ROM и DVD диски, дискеты, переносные (WPD) устройства, порты, принтеры и.т.д.). Доступ регулируется по разрешениям чтения, записи и исполнения.

Подсистема состоит из ММС оснастки управления и ядровой компоненты.

3.5. Подсистема мандатного шифрования

Подсистема мандатного шифрования реализует возможность административного управления шифрованием данными, сохраняемыми пользователем на съемные носители информации или считываемые пользователем со съемных носителей информации (7).

Подсистема состоит из ММС оснастки управления и ядровой компоненты.

3.6. Подсистема контроля исполнения сценариев

Подсистема контроля исполнения сценариев реализует возможность создания списка сценариев разрешенных к исполнению.

Подсистема состоит из ММС оснастки управления и модулей фильтрации выполнения сценариев различного типа.

Список литературы

1. **ФСБ России.** Требования по защите конфиденциальной информации от несанкционированного доступа в автоматизированных информационных системах, расположенных на территории Российской Федерации.

2. **Компания "СиЭйЭн".** Руководство администратора безопасности. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 01.

3. —. Руководство администратора безопасности. Установка. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 02.

4. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 03.

5. —. Руководство администратора безопасности. Политики управления приложениями. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 04.

6. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 05.

7. —. Мандатное шифрование. Концепция. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 91 01.

8. —. Описание применения. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 31 01.

9. —. Руководство пользователя. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 34 01.

10. —. Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 30 01.