Средство защиты информации

«КриптоПро SPR»

Версия 4.0

Руководство администратора безопасности

Аудит

ЖТЯИ.00112-01 90 05

Листов 12

Компания «КРИПТО-ПРО»

2021

ООО «КРИПТО-ПРО»
Адрес 127018, г. Москва, ул. Сущевский Вал, дом 18
Телефон +7 (495) 995-4820
e-mail info@cryptopro.ru
Web www.cryptopro.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. Введение

Данное руководство предназначено для администраторов средства защиты информации «КриптоПро SPR» версия 4.0 (сокращенные названия изделия – SPR 4.0). В руководстве содержатся сведения, необходимые администраторам для настройки и управления основными механизмами защиты.

2. Основные подсистемы

Функционирование СЗИ SPR 4.0 опирается на следующие подсистемы:

- Подсистема управления политиками;
- Подсистема доверенной аутентификации;
- Подсистема дискреционного разграничения доступа;
- Подсистема защиты критических ресурсов;
- Подсистема контроля доступа к устройствам;
- Подсистема мандатного шифрования;
- Подсистема замкнутой программной среды;
- Подсистема контроля запуска сценариев;
- Подсистема аудита безопасности.

Данное Руководство описывает порядок настройки следующих политик безопасности основных подсистем, реализуемых СЗИ SPR 4.0:

- Подсистема аудита безопасности.

Описание порядка настройки политик безопасности, не входящих в данное Руководство, содержится в соответствующих документах в составе документации [1], [2], [3] и [4].

3. Управление аудитом событий СЗИ SPR 4.0

При первоначальной установке средства защиты информации «КриптоПро SPR» версия 4.0 регистрируется отдельные провайдеры событий для каждой из подсистем в разделе «Журналы приложений и служб»:

- CryptoPro-SPR-CriticalResourceProtection – для подсистемы защиты критических ресурсов.
- CryptoPro-SPR- DevicesAccessControl – для подсистемы управления доступа к устройствам
- CryptoPro-SPR-EnchancedEfsPolicies – для подсистемы расширенных политик EFS.

Журналы приложений и служб используются приложениями и службами для регистрации событий, связанных с их работой. Для управления журналами событий можно использовать оснастку «Просмотр событий» или программу командной строки «wevtutil».

В ОС Windows 7 и более старших инфраструктура, обеспечивающая регистрацию событий, основана на формате XML. Данные о каждом событии соответствуют XML-схеме, что позволяет получить доступ к XML-коду любого события. Кроме того, можно создавать основанные на XML запросы для получения данных из журналов. Оснастка «Просмотр событий» предоставляет простой графический интерфейс для доступа к этим возможностям.

При первоначальной установке SPR 4.0 список правил защиты каждой политики безопасности пуст, поэтому активация политик не приводит к блокировке модификации каких-либо областей файловой системы. Все политики SPR 4.0 включены в режиме «Аудит» - дополнительных

действий для активации сбора событий подсистем, входящих в состав средства защиты информации SPR 4.0 не требуется.

3.1. События подсистемы защиты критических ресурсов

Имя канала: CryptoPro-SPR-CriticalResourceProtection

Таб. 1. События подсистемы защиты критических ресурсов

ID	Канал	Уровень	Описание
100	Admin	Информация	Запущен цикл расчета контрольных сумм защищаемых файлов.
101	Admin	Информация	Завершен цикл расчета контрольных сумм защищаемых файлов. Информация о цикле: Обработанные файлы: %1 Ошибки: %2
102	Admin	Информация	Запущен цикл проверки контрольных сумм защищаемых файлов.
103	Admin	Информация	Завершен цикл проверки контрольных сумм защищаемых файлов. Информация о цикле: Проверенные файлы: %1 Нарушение целостности: %2 Ошибки:%3
104	Admin	Информация	Выполнена попытка получения доступа к аудируемому объекту. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6 Сведения о запросе на доступ: Маска доступа: %7 Доступ: %8
105	Admin	Информация	Выполнена попытка создания объекта файловой системы типа hard link, который ссылается на аудируемый объект. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе:

			Идентификатор: %4 Имя файла: %6
106	Admin	Предупреждение	Выполнена попытка получения доступа к защищаемому объекту. В соответствии с настройками политик доступ запрещен. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6 Сведения о запросе на доступ: Маска доступа: %7 Доступ: %8
107	Admin	Предупреждение	Выполнена попытка создания объекта файловой системы типа hard link, который ссылается на защищаемый объект. В соответствии с настройками политик доступ запрещен. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6

3.2. События подсистемы управления доступа к устройствам

Имя источника: CryptoPro-SPR-DevicesAccessControl

Таб. 2. События подсистемы управления доступом к устройствам

ID	Канал	Уровень	Описание
200	Operational	Информация	Активировано контролируемое устройство. Сведения об устройстве: Класс: %2 Тип шины: %4 Описание: %6 Экземпляр: %8
201	Operational	Информация	Контролируемое устройство удалено. Сведения об устройстве: Класс: %2 Описание: %4 Экземпляр: %6
202	Operational	Информация	Смонтирован том на контролируемом съемном носителе. Сведения о томе: Имя: %2 Метка: %4 Файловая система: %5 Экземпляр: %7
203	Operational	Информация	Размонтирован том на контролируемом съемном носителе. Сведения о томе: Класс: %1 Экземпляр: %2 Описание: %3
204	Admin	Информация	Выполнена попытка получения доступа к аудируемому устройству. Сведения об устройстве: Класс: %2 Описание: %4 Экземпляр: %6 Сведения о процессе: Идентификатор: %7 Имя файла: %9 Сведения о запросе на доступ: Маска доступа: %10

			Доступ: %11
205	Admin	Информация	Выполнена попытка получения доступа к объекту файловой системы на аудируемом устройстве. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6 Сведения о запросе на доступ: Маска доступа: %7 Доступ: %8
206	Admin	Ошибка	Выполнена попытка получения доступа к контролируемому устройству. В соответствии с настройками политик доступ запрещен. Сведения об устройстве: Класс: %2 Описание: %4 Экземпляр: %6 Сведения о процессе: Идентификатор: %7 Имя файла: %9 Сведения о запросе на доступ: Маска доступа: %10 Доступ: %11
207	Admin	Ошибка	Выполнена попытка получения доступа к объекту файловой системы на контролируемом устройстве. В соответствии с настройками политик доступ запрещен. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6 Сведения о запросе на доступ: Маска доступа: %7 Доступ: %8

3.3. События подсистемы расширенных политик EFS.

Имя источника: CryptoPro-SPR-EnchancedEfsPolicies.

Таб. 3. События подсистемы расширенных политик EFS.

ID	Канал	Уровень	Описание
300	Admin	Информация	Выполнена попытка получения доступа к незашифрованному файлу на аудируемом устройстве. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6 Сведения о запросе на доступ: Маска доступа: %7 Доступ: %8
301	Admin	Ошибка	Выполнена попытка получения доступа к незашифрованному файлу на контролируемом устройстве. В соответствии с настройками политик доступ запрещен. Сведения об объекте: Тип: %1 Имя: %3 Сведения о процессе: Идентификатор: %4 Имя файла: %6 Сведения о запросе на доступ: Маска доступа: %7 Доступ: %8

Список литературы

1. **Компания "КРИПТО-ПРО".** Руководство администратора безопасности. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 01.

2. —. Руководство администратора безопасности. Установка. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 02.

3. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 03.

4. —. Руководство администратора безопасности. Политики управления приложениями. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 04.

5. —. Формуляр. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 30 01.