Средство защиты информации

«КриптоПро SPR»

Версия 4.0

Описание применения

ЖТЯИ.00112-01 31 01

Листов 22

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 4
1. Назначение программы 5
2. Основные технические характеристики 7
3. Условия применения 9
3.1. Требования к аппаратным средствам 9
3.2. Требования к установке и эксплуатации 9
4. Описание задачи 12
4.1. Подсистемы SPR 4.0 12
4.1.1. Схема управления подсистемами 12
4.1.2. Подсистема доверенной аутентификации 13
4.1.3. Подсистема дискреционного разграничения доступа 15
4.1.4. Подсистема защиты критических ресурсов 19
4.1.5. Подсистема контроля доступа к устройствам 19
4.1.6. Подсистема мандатного шифрования 19
4.1.7. Подсистема замкнутой программной среды 20
4.1.8. Подсистема аудита безопасности 20
Список литературы 22

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 «КриптоПро SPR» версия 4.0 (сокращенное названия изделия – SPR 4.0) предназначено для обеспечения защиты информационных ресурсов АИС, состоящих из АРМ и серверов, функционирующих под управлением ОС компании Microsoft (Таб. 1), и совместно с другими средствами защиты усиливает штатные механизмы ОС, обеспечивающие информационную безопасность АИС.

Таб. 1. Операционные системы, поддерживаемые SPR 4.0 (исполнения 1, 2)

Выпуски	Версия	Канал обслуживания	Тип	Минимальная рекомендуемая сборка	Метод активации
Windows 10 Pro Pro N	20H2	SAC	32-bit	19042.631	Retail
Windows 10 Pro Pro N Pro for Workstation Pro for Workstation N	20H2	SAC	64- bit	19042.631	Retail
Windows 10 Pro Pro N Enterprise Enterprise N	20H2	SAC	32- bit	19042.746	Volume
Windows 10 Pro Pro N Pro for Workstation Pro for Workstation N Enterprise Enterprise N	20H2	SAC	64- bit	19042.746	Volume
Windows 10 LTSC 2019 Enterprise Enterprise N	1809	LTSC	64- bit	17763.1757	Volume

Windows Server Standard (Server Core) Datacenter (Server Core)	20H2	SAC	64- bit	19042.631	Volume
Windows Server 2016 Standard Standard (Server Core) Datacenter Datacenter (Server Core)	1607	LTSC	64- bit	14393.4225	Volume
Windows Server 2019 Standard Standard (Server Core) Datacenter Datacenter (Server Core)	1809	LTSC	64- bit	17763.1757	Volume

Примечания: 1. Все выпуски ОС поддерживаются в вариантах на английском и русском языках.
2. Порядок и сроки эксплуатации ОС определяются производителем ОС

2. Основные технические характеристики

SPR 4.0 поставляется в восьми исполнениях.

ОС Microsoft Windows (Таб. 1) со встроенными и дополнительными интегрированными механизмами обеспечения безопасности, реализуемыми SPR 4.0 (исполнение 1), обеспечивает уровень защиты АК3 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 событий подсистем безопасности СЗИ SPR 4.0.
- 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, 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).

ОС Microsoft Windows (Таб. 1) со встроенными и дополнительными интегрированными механизмами обеспечения безопасности, реализуемыми SPR 4.0 (исполнение 2) обеспечивает уровень защиты АК2 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 событий подсистем безопасности СЗИ SPR 4.0.
- 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, 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).

3. Условия применения

SPR 4.0 эксплуатируется в составе АИС, состоящих из АРМ и серверов, функционирующих под управлением ОС компании Microsoft (Таб. 1). На всех АРМ в составе АИС должен быть установлен и настроен экземпляр СЗИ SPR 4.0.

3.1. Требования к аппаратным средствам

Требования к аппаратным средствам приведены в таблицах Таб. 2 - Таб. 3.

Таб. 2. Системные требования для ОС Microsoft Windows 10

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

Таб. 3. Минимальные системные требования для ОС Microsoft Windows Server 2016/2019

Компонент	Требование
Компьютер и процессор	1,4 ГГц (процессор с архитектурой x64).
Память	512 МБ 2 ГБ для варианта установки "Сервер с рабочим столом".
Жесткий диск	32 ГБ.
Сетевой адаптер	Адаптер Ethernet с пропускной способностью не менее 1 ГБ Совместимость со спецификацией архитектуры PCI Express

3.2. Требования к установке и эксплуатации

Для обеспечения защиты информации при эксплуатации SPR 4.0 необходимо соблюдение следующих общих условий применения:

- Установка и настройка SPR 4.0 должна производиться в соответствии с [1], [2], [3], [4] и [5].

- 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 4.0 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.
- Все используемые диски съемных устройств хранения должны быть предварительно отформатированы с использованием файловой системы NTFS.
- Общий доступ к объектам файловой системы, расположенным на дисках съемных устройств хранения, должен быть запрещен.
- На всех АРМ должны быть заблокированы порты IEEE 1394 (Firewire).
- СКЗИ, входящее в состав SPR 4.0, 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.

Штатная работа СЗИ SPR 4.0 может быть нарушена вследствие неправильной инициализация СЗИ при старте системы, несанкционированного изменения настроек и кода исполняемых модулей СЗИ, а также направленного воздействия со стороны привилегированных процессов и непривилегированных процессов, осуществивших эскалацию привилегий с использованием уязвимостей в операционной системе и процессах, выполняющихся от привилегированных учетных записей.

Указанные угрозы могут быть реализованы посредством загрузки сторонней операционной системы. Для обеспечения невозможности загрузки сторонней операционной системы, а также корректности загрузки штатной операционной системы хранилище BCD ОС Windows при установке SPR 4.0 должно быть настроено таким образом, чтобы исключить запуск Windows в ином режиме, кроме режима по умолчанию. Для этого в хранилище BCD должна быть задана единственная запись для загрузчика операционной системы, в записи параметр «recoveryenabled» должен быть удален. Записи для приложений должны отсутствовать.

К некорректной загрузке SPR 4.0 также может привести изменение бинарных модулей, формирующих стартовый образ операционной системы для запуска «Ntoskrnl», а также настроек этих модулей. С учетом отсутствия возможности стартового контроля целостности указанных модулей и их настроек средствами СЗИ, данная угроза должна быть блокирована иными средствами.

4. Описание задачи

Интеграция механизмов обеспечения безопасности SPR 4.0 в ОС Microsoft Windows (Таб. 1) и их использование совместно с базовыми механизмами позволяет обеспечить общий уровень защиты ОС до АК3.

SPR 4.0 интегрируется в ОС Microsoft Windows (Таб. 1) как ее часть и базируется на документированных механизмах защиты информации ОС, что обеспечивает высокую устойчивость работы и совместимость с другими программными продуктами.

4.1. Подсистемы SPR 4.0

Функционирование 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.

4.1.1. Схема управления подсистемами

Общая схема управления подсистемами SPR 4.0 приведена на Рис. 1.

Управления политиками SPR 4.0 осуществляется посредством MMC оснасток, интегрированных в системную оснастку «Параметры безопасности». Это позволяет администратору безопасности управлять всеми политиками безопасности, включая политики SPR 4.0, из одной консоли.

Параметры, установленные администратором безопасности в оснастках SPR 4.0, 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 4.0.

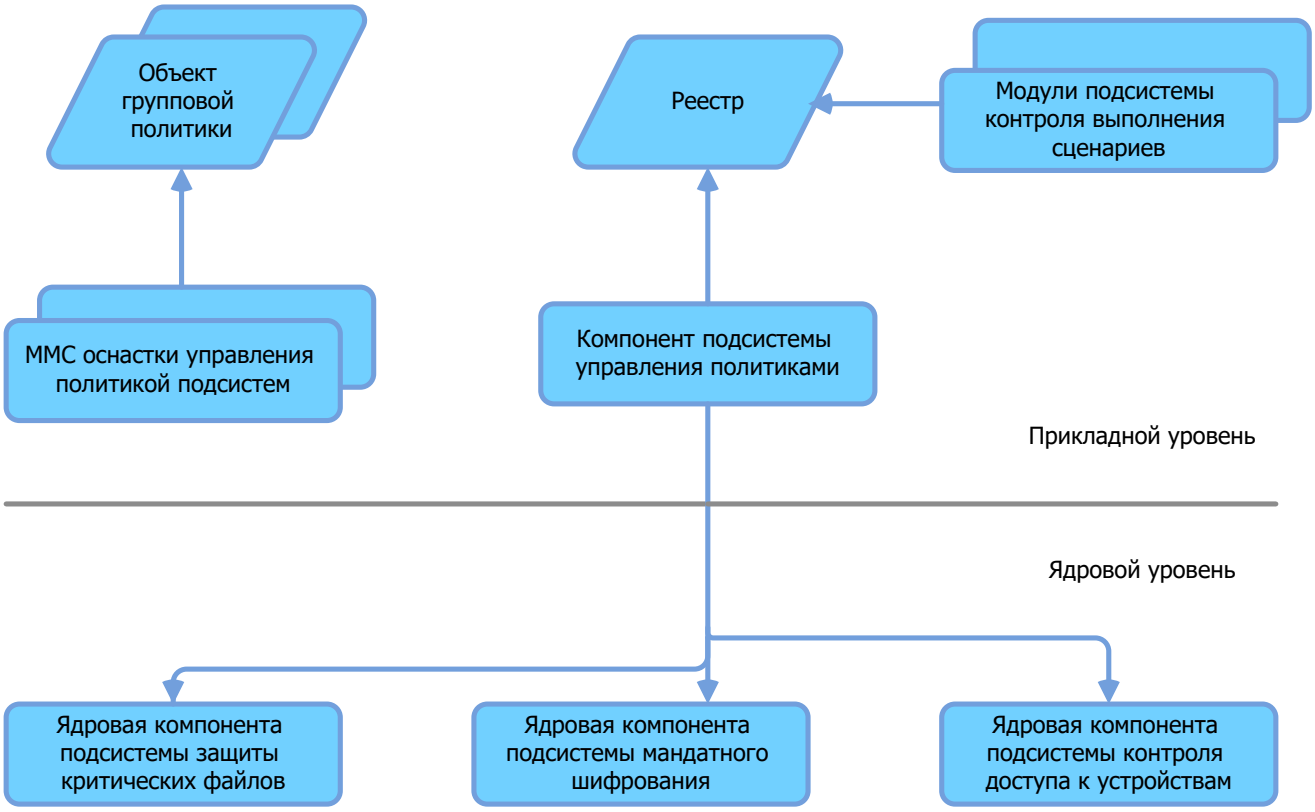

Рис. 1 Общая схема управления подсистемами SPR 4.0

4.1.2.Подсистема доверенной аутентификации

Подсистема доверенной аутентификации SPR 4.0 реализует возможность аутентификации пользователей в домене на основе российских криптографических стандартов.

Подсистема доверенной аутентификации SPR 4.0 базируется на подсистеме идентификации и аутентификации ОС Microsoft Windows и дополняется продуктом компании КриптоПро Winlogon. Winlogon является доверенным процессом, отвечающим за управление взаимодействий с пользователем, связанных с безопасностью. Им координируются вход в систему, запуск первого процесса пользователя при входе в систему, обработка выхода из системы и управление рядом других операций, относящихся к безопасности, включая запуск LogonUI для ввода паролей при входе в систему, изменении паролей, блокировке и разблокировке рабочей станции. Процесс Winlogon гарантирует, что операции, связанные с безопасностью, невидимы любым другим активным процессам. Например, Winlogon гарантирует, что не пользующийся доверием процесс не может получить управление рабочим столом в ходе одной из таких операций, получив тем самым доступ к паролю. Winlogon при получении имени и пароля учетной записи пользователя зависит от установленных в системе поставщиков учетных записей.

Аутентификация построена на следующих ключевых понятиях:

- инфраструктура аутентификации;
  набор серверов аутентификации и доверенных центров аутентификации, реализующих сервисы управления аутентификацией.

- сервера аутентификации;

  физические машины, обеспечивающие исполнение функций аутентификации.

- доверенный орган аутентификации;
  логическое понятие органа, являющегося доверенными с точки зрения пользователей для реализации функций аутентификации. Физически, доверенные орган аутентификации представляет собой один или несколько серверов аутентификации. В терминах Windows, домен является доверенным органом аутентификации, а контроллер домена (domain controller - DC) – физическим сервером аутентификации.
- аутентификационные данные.
  идентификатор (ID) и пароль, предоставляемые пользователем доверенному органу аутентификации. В зависимости от типа аутентификационных данных, пользователь может просто запомнить их (например, ID пользователя и пароль) или сохранить аутентификационные данные на каких-либо носителях (например, интеллектуальной карте). Биометрические аутентификационные данные основываются на физических или поведенческих характеристиках пользователя.

База аутентификационных данных является хранилищем доверенного органа аутентификации, где в безопасном формате хранятся копии аутентификационные данных пользователей и компьютеров. Аутентификационный токен является доказательством подлинности аутентификации и используется для доступа к ресурсам в области ответственности доверенного органа аутентификации. Токен выдается пользователю или компьютеру доверенным органом аутентификации после успешной аутентификации. В стандартном процессе аутентификации пользователь отправляет результат криптографической операции над своими аутентификационными данными в доверенный орган аутентификации. Доверенный орган аутентификации проверяет аутентификационные данные, используя данные, хранящиеся в его базе. Если аутентификационные данные, предоставленные пользователем, и данные, хранящиеся в базе, соответствуют, или если результат криптографической операции над аутентификационные данными, хранящимися в базе эквивалентен результату, предоставленному пользователем, личность пользователя, считается подтвержденной. В результате, пользователю предоставляется или запрещается доступ к области ответственности доверенного органа аутентификации. Чтобы доказать, что пользователь успешно прошел аутентификацию, доверенный орган аутентификации выдает пользователю криптографический токен. Этот токен используется в качестве доказательства успешной аутентификации при последующем доступе к другим ресурсам в области ответственности доверенного органа аутентификации, например, при доступе к файл-серверу.

Программный продукт КриптоПро Winlogon обеспечивает взаимную аутентификацию пользователя в домене. В качестве механизма аутентификации используется предъявление пользователем ключевого носителя на основании сертификата его открытого ключа.

Архитектура подсистемы интерактивной аутентификации реализует наиболее распространенный и наиболее безопасный способ интерактивного входа с использованием "безопасного входа" или "классического входа" (Secure Attention Sequence - SAS). В этом случае, процесс аутентификации начинается всякий раз, когда пользователь инициирует SAS для входа на локальный компьютер или в домен. Winlogon является компонентом ОС, который управляет взаимодействием с пользователем, в части касающейся безопасности, в том числе интерактивной аутентификацией. Credential Providers – набор компонентов, отвечающих за интерактивное взаимодействие с пользователем через интерфейс входа в систему, извлечения учетных данных пользователя, и передачи их Local Security Authority (LSA).

LSA является компонентом ОС, который действует как локальный доверенный орган аутентификации. Для проверки аутентификационных данных пользователя, LSA взаимодействует с библиотеками Authentication Packages (AP) и Security Support Providers (SSP). Библиотеки AP и SSP, в свою очередь, обращаются к базе аутентификационных данных для проверки данных пользователя. Библиотеки kerberos.dll и msv1_0.dll являются реализациями библиотек SSP/AP: библиотека MSV1_0 реализует протокол NTLM версии 1 и 2, библиотека MSV1_0 включает в себя логику сквозной аутентификации NTLM (сквозная аутентификации NTLM реализуется, если не доступна доменная базы данных аутентификации).

4.1.3.Подсистема дискреционного разграничения доступа

Подсистема дискреционного разграничения доступа обеспечивает контроль прав доступа субъекта к объекту доступа. Работа механизма дискреционного доступа заключается в защите объектов и в регистрации доступа. В число защищаемых в Windows объектов входят файлы, устройства, почтовые ящики, каналы (именованные и безымянные), задания, процессы, потоки, события, ключевые события, пары событий, мьютексы, семафоры, общие разделы памяти, порты завершения ввода-вывода, LPC-порты, таймеры ожиданий, маркеры доступа, тома, станции окон, рабочие столы, сетевые ресурсы, службы, разделы реестра, принтеры, объекты Active Directory и т. д.

Система безопасности должна сначала убедиться в идентичности каждого пользователя. Такая необходимость гарантии пользовательской идентичности является причиной того, что ОС Windows требует аутентификации входа в систему перед получением доступа к любым системным ресурсам. Таким образом, подсистема дискреционного разграничения доступа опирается на подсистему доверенной аутентификации.

Модель безопасности ОС Windows требует, чтобы поток, прежде чем открыть объект, указал, какого типа действия он хочет совершить над объектом. Для выполнения проверок прав доступа, основанных на желаемом потоком доступе, диспетчер объектов вызывает SRM, и если доступ предоставляется, процессу потока назначается дескриптор, с которым поток (или другие потоки процесса) может выполнять дальнейшие операции над объектом. Сутью модели безопасности SRM является уравнение, имеющее три входных параметра: идентификационные данные безопасности потока, доступ, который поток желает получить к объекту, и настройки безопасности объекта. На

выходе получаем либо «да», либо «нет», что показывает, дает модель безопасности потоку запрошенный доступ или не дает.

Одним из событий, заставляющих диспетчер объектов выполнять проверку безопасности доступа, является открытие процессом существующего объекта с использованием его имени. Когда объект открывается по имени, диспетчер объектов выполняет поиск указанного объекта в пространстве имен диспетчера объектов.

Еще одним событием, заставляющим диспетчер объектов проводить проверку прав доступа, является ссылка процесса на объект с использованием существующего дескриптора. Такие ссылки зачастую проводятся опосредованно, например, когда процесс вызывает API-функцию Windows для работы с объектом и передает ей дескриптор объекта. Например, поток, открывающий файл, может запросить право на чтение файла. Если у потока есть право на такой доступ к объекту, как предписано его контекстом безопасности и настройками безопасности файла, диспетчер объектов создает дескриптор, который представляет файл в таблице дескрипторов того процесса, которому принадлежит поток. Типы доступа предоставляются процессу через дескриптор, который хранится с дескриптором диспетчера объектов.

Функции безопасности Windows также позволяют Windows-приложениям определять свои собственные закрытые объекты и вызывать службы SRM (через API-функции пользовательского режима AuthZ, которые будут рассмотрены чуть позже), чтобы задействовать модель безопасности Windows в отношении таких объектов. Многие функции режима ядра, которые диспетчер объектов и другие компоненты исполняющей системы используют для защиты своих собственных объектов, экспортируются в виде API-функций Windows, работающих в пользовательском режиме. Таким образом, Windows приложения могут воспользоваться гибкостью модели безопасности и явным образом интегрироваться с имеющимися в Windows интерфейсами аутентификации и администрирования.

Вместо использования имен для идентификации всех действий в ОС Windows используются идентификаторы безопасности — security identifiers (SID). SID идентификаторы имеются у пользователей, а также у локальных и доменных групп, у локальных компьютеров, доменов, участников доменных групп и служб. SID представляет собой числовое значение переменной длины, состоящее из номера версии SID-структуры, 48-разрядное значение идентификатора полномочий и переменное количество 32-разрядных кодов значений подчиненных полномочий или относительных идентификаторов — relative identifier (RID). Значение полномочий идентифицирует агента, выдавшего SID, и этим агентом обычно является локальная система Windows или домен. Значения подчиненных полномочий идентифицируют представителей, имеющих отношение к выдавшему полномочия, а RID-идентификаторы являются просто способом, применяемым в Windows для создания уникальных SID на основе общего базового SID. Из-за большой длины SID-идентификаторов Windows старается сгенерировать внутри каждого SID понастоящему случайное значение, практически невозможно, чтобы Windows выдала один и тот же SID на машине или домене, или где-либо еще дважды.

Windows выдает SID-идентификаторы, которые состоят из SID компьютера или домена с предопределенным RID-идентификатором для множества предопределенных учетных записей и групп. Например, RID для учетной записи администратора имеет значение 500, а RID для гостевой учетной записи имеет значение 501. Например, учетная запись локального администратора имеет в своей основе SID компьютера с добавленным к нему RID, который имеет значение 500: S-1-5-21-13124455-12541255-61235125-500.

Windows также определяет ряд встроенных локальных и доменных SID для представления широко известных групп. Например, SID, идентифицирующий любые учетные записи (за исключение анонимных пользователей), является всеобщим — Everyone SID: S-1-1-0. Другим примером группы, которая может быть представлена SID-идентификатором, является сетевая группа, то есть группа, представляющая пользователей, зарегистрировавшихся на машине по сети. SID сетевой группы имеет значение S-1-5-2. В представленной ниже табл. 6.2 из документации по Windows SDK показываются некоторые основные, широко известные SID-идентификаторы, их числовые значения и использование. В отличие от пользовательских SID эти SID-идентификаторы являются предопределенными константами и имеют одинаковые значения на каждой системе Windows и домене во всем мире. Таким образом, файл, доступный членам группы Everyone на той системе, где он был создан, также будет доступен группе Everyone на любой другой системе или домене, на которую будет перемещен жесткий диск, на котором он размещается. Разумеется, пользователи на таких системах должны пройти аутентификацию учетной записи на этих системах, перед тем как стать членами группы Everyone.

И наконец, Winlogon создает уникальный SID входа в систему для каждого интерактивного сеанса входа. Обычно SID входа в систему применяется в элементе управления доступом — access control entry (ACE), который разрешает доступ во время сеанса входа клиента в систему. Например, служба Windows для запуска нового сеанса входа в систему может использовать функцию LogonUser. Эта функция возвращает маркер доступа, из которого служба может извлечь SID входа в систему. Затем эта служба может использовать SID в ACE, позволяющем сеансу входа клиента в систему получать доступ к интерактивной станции окна и к рабочему столу. SID для сеанса входа в систему имеет значение S-1-5-5-0, RID генерируется случайным образом.

Для идентификации контекста безопасности процесса или потока SRM использует объект под названием маркер доступа. Контекст безопасности состоит из информации, описывающей учетную запись, группы и привилегии, связанные с процессом или потоком. Маркеры также включают такую информацию, как ID сеанса, уровень целостности и состояние виртуализации UAC. При выполнении процесса входа в систему процесс LSASS создает исходный маркер для представления пользователя, входящего в систему. Затем он определяет, относится ли пользователь к группе, имеющей высокие полномочия, или обладает ли он высокими привилегиями.

Для определения доступности объектов и вида защищаемых операций, имеющиеся в ОС Windows механизмы безопасности используют два компонента. Один компонент включает в себя принадлежащий маркеру SID учетной записи пользователя и поля SID групп. Монитор безопасности

— security reference monitor (SRM) использует SID-идентификаторы для определения, может ли процесс или поток получить запрашиваемый доступ к защищаемому объекту, например, к NTFS-файлу.

Маркеры, идентифицирующие учетные данные пользователя, являются только лишь частью уравнения, определяющего безопасность объекта. Другой частью уравнения является информация безопасности, связанная с объектом, которая определяет, кто и какие действия с объектом может выполнять. Структура данных для этой информации называется дескриптором безопасности. В дескриптор безопасности входят следующие атрибуты:

- Номер версии;
  Версия модели безопасности SRM, использованная для создания дескриптора.
- Флаги;
  Дополнительные модификаторы, определяющие поведение или характеристики дескриптора. Эти флаги перечислены в табл. 6.5.
- SID владельца;
  Идентификатор безопасности владельца
- SID группы;
  Идентификатор безопасности основной группы объекта (используется только подсистемой POSIX)
- Избирательный список управления доступом — Discretionary access control list (DACL);
  Указывает, кто и какой доступ имеет к объекту
- Системный список управления доступом — System access control list (SACL);
  Указывает, какие операции какими пользователями должны регистрироваться в журнале аудита безопасности и конкретный уровень целостности объекта.

В DACL в каждом ACE-элементе содержится SID и маска доступа, которая обычно определяет права доступа (чтение, запись, удаление и т. д.), предоставленные или запрещенные держателю SID. Существует девять типов ACE-элементов, которые могут появляться в DACL:

- доступ разрешен;
- доступ запрещен;
- объект разрешен;
- объект запрещен;
- обратный вызов разрешен;
- обратный вызов запрещен;
- обратный вызов объекта разрешен;
- обратный вызов объекта запрещен;
- условные требования.

Аккумулирование прав доступа, предоставленных отдельными ACE-элементами, формирует набор прав доступа, предоставленных ACL-списком. Если в дескрипторе безопасности отсутствует

DACL (то есть имеется нулевой DACL), полный доступ к объекту предоставляется кому угодно. Если DACL пуст (то есть в нем нуль ACE-элементов), никто не имеет доступа к объекту.

4.1.4.Подсистема защиты критических ресурсов

Подсистема защиты критических ресурсов SPR 4.0 реализует контроль целостности объектов файловой системы. Механизм контроля целостности осуществляет слежение за неизменностью контролируемых объектов файловой системы (ФС). Контроль проводится в автоматическом режиме в соответствии с заданной периодичностью с момента загрузки ОС. В штатном режиме работы подсистема защиты критических ресурсов SPR 4.0 обеспечивает запрет на модификацию объектов ФС, стоящих на контроле, с использованием драйвера-фильтра. Описание работы подсистемы защиты критических ресурсов SPR 4.0 представлено в [1].

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.

4.1.5.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. Описание работы подсистемы контроля доступа к устройствам SPR 4.0 представлено в [1].

Подсистема состоит из ММС оснастки управления и ядровой компоненты.

4.1.6.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 [6].

Подсистема состоит из ММС оснастки управления и ядровой компоненты.

4.1.7. Подсистема замкнутой программной среды

Подсистема замкнутой программной среды позволяет администраторам ограничивать запуск пользователями нежелательных или ненадежных приложений на серверах и рабочих станциях, работающих как в сценарии управления домена, так и в среде рабочей группы.

Ограничение запуска может быть установлено для следующих категорий (коллекций) объектов:

- правила исполняемых файлов;
- правила установщика Windows;
- правила сценариев;
- правила DLL.

В каждой коллекции можно создать правила на основании трех критериев:

- правила для пути ФС к объекту;
  разрешен запуск только тех файлов, которые находятся внутри определенного дерева каталогов. Этот критерий может также использоваться для идентификации конкретных файлов.
- правила для полей сертификата ОК подписи кода;
  позволяет составлять различные комбинации из имени издателя, имени продукта, имени файла и версии, разрешая выполнение подписанного объекта
- правила для хэш-значения объекта.
  позволит обнаружить внесение в файл изменений и помешать его запуску, что также может рассматриваться как недостаток, если файлы часто подвергаются изменениям, поскольку правило на основе хэша нужно будет часто обновлять.

Одним из режимов работы AppLocker является режим аудита, позволяющий администратору создавать политику AppLocker и проверять результаты (хранящиеся в системном журнале событий) для определения, будет ли политика выполняться, как ожидалось, фактически не накладывая ограничений. Режим аудита AppLocker может использоваться для отслеживания того, какие приложения используются одним или несколькими пользователями системы. Описание работы подсистемы замкнутой программной среды представлено в [4].

Подсистема состоит из MMC оснастки управления (в составе консоли управления Групповой политикой) и ядровой компоненты (служба «AppIDSvc»).

4.1.8. Подсистема аудита безопасности

Подсистема аудита безопасности генерирует события аудита в качестве результата проверки доступа. Политика аудита локальной системы управляет решением на аудит конкретного типа события безопасности. Политика аудита, также называемая локальной политикой безопасности, настраивается с помощью редактора локальной политики безопасности.

Важной областью применения механизма аудита является ведение журнала доступов к защищенным объектам, в частности к файлам. Для этого должна быть включена политика Аудит доступа к объектам (Audit Object Access) и в системных списках управления доступом должны быть ACE-элементы аудита, разрешающие проведение аудита заданных объектов.

Записи аудита доступа к объекту включают не только сам факт разрешенного или запрещенного доступа, но также и причину успеха или отказа. Эта «причина для доступа», дающая отчет в общем виде, принимает в записи аудита форму записи управления доступом.

В дополнение к элементам доступа к объектам, применяемым в отношении отдельных объектов, в отношении системы может быть определена глобальная политика аудита, позволяющая проводить аудит доступа к объекту для всех объектов файловой системы, для всех разделов реестра или и к тем и к другим. Поэтому администратор безопасности может быть уверен, что нужный аудит будет выполнен без необходимости установки или изучения списков SACL у всех отдельных заданных объектов. Описание работы подсистемы аудита SPR 4.0 представлено в [5].

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. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 05.

6. —. Мандатное шифрование. Концепция. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 91 01.

7. —. Описание применения. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 31 01.

8. —. Руководство пользователя. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 34 01.

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