Средство защиты информации

«КриптоПро SPR»

Версия 4.0

Мандатное шифрование

Концепция

ЖТЯИ.00112-01 91 01

Листов 8

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

В настоящее время одной из самых распространенных проблем в области безопасности информации корпоративных компьютерных систем является контроль над использованием съемных носителей информации.

Случаи утери (кражи) съемных носителей с конфиденциальной информацией, случаи использование съемных носителей для злонамеренного выноса больших объемов информации, распространение вирусов и закладок через съемные носители являются в настоящее время серьезными угрозами безопасности корпоративных сетей.

В настоящее время в области контроля над использованием съемных носителей информации имеются два основных подхода.

Первый подход представляет собой полный запрет на использования съемных носителей информации внутри корпоративного сегмента. Часто это реализуется путем физической блокировки USB или FireWire портов.

При втором подходе используются решения, позволяющие управлять доступом к съемным носителям. Примером реализации данного подхода служит подсистема Windows Removable Storage Access, реализованная в ОС Windows начиная с Windows Vista.

В системе защиты информации на съемных носителях, получившей название SPR Device Security, совмещен как традиционных подход управления доступом к устройствам, так и реализован новый подход к защите информации на съемных носителях.

2. Расширенные политики EFS

Новый подход, предложенный компанией КРИПТО-ПРО, основан на использовании подсистемы файлового шифрования ОС Microsoft Windows Encrypting File System (далее - EFS). Реализуемая в рамках данного подхода подсистема названа Расширенные политики Шифрующей Файловой Системы (Enhanced Encrypting File System (EFS) Policies) (далее - EFP).

Принцип предложенного подхода состоит в том, чтобы не ограничивать пользователей корпоративной сети в возможности физического использования съемных носителей информации. Однако при этом Администратору предоставляется возможность мандатного управления атрибутами шифрования файлов (далее - мандатное шифрование) на съемных носителях информации. Термин мандатное (обязательное) шифрование означает, что необходимость шифрования информации на съемном носителе определяется администратором, а не желанием или не желанием пользователя.

По умолчанию, все пользователи имеют разрешение работать только с зашифрованной информацией. Для того чтобы пользователь получил доступ (на чтение, запись, исполнение) к незашифрованной информации администратор должен дать ему разрешение соответствующее

разрешение. В рамках управления мандатным шифрованием определяется три типа разрешений (permissions), которые администратор может назначить пользователям:

Разрешение читать незашифрованные файлы со съемных носителей информации. Данное разрешение дает пользователю право открывать на чтение файлы, находящиеся на съемном носителе информации, и не зашифрованные с помощью EFS.

Разрешение создавать незашифрованные файлы и записывать в незашифрованные файлы на съемных носителях информации. Данное разрешение дает пользователю возможность создавать на съемных носителях информации файлы, не зашифрованные с помощью EFS. Также данное разрешение дает пользователю возможность открывать на запись файлы, находящиеся на съемном носителе информации, и не зашифрованные с помощью EFS.

Разрешение исполнять незашифрованные файлы со съемных носителей информации. Данное разрешение дает пользователю право открывать на исполнение файлы, находящиеся на съемном носителе информации, и не зашифрованные с помощью EFS.

Таким образом, устанавливая данные разрешения, администратор имеет возможность создать «белый» список пользователей, которым разрешены те или иные операции с незашифрованными файлами на съемных носителях информации.

Пользователи, не внесенные в разрешительные списки, имеют право проводить соответствующие файловые операции только с зашифрованными с помощью EFS файлами:

1. Пользователи, не имеющие разрешения читать незашифрованные файлы со съемных носителей информации, имеют право открывать на чтение файлы, находящиеся на съемном носителе информации, только зашифрованные с помощью EFS.
2. Пользователи, не имеющие разрешения создавать незашифрованные файлы на съемных носителях информации, имеют право создавать файлы на съемных носителях, но при этом вновь созданные файлы будут зашифрованы с помощью EFS. Установка атрибута шифрования происходит в прозрачном режиме. Также пользователи, не имеющие разрешения записывать данные в незашифрованные файлы, имеют право открывать на запись только файлы, зашифрованные с помощью EFS.
3. Пользователи, не имеющие разрешения исполнять незашифрованные файлы со съемных носителей информации, имеют право открывать на исполнение только файлы, зашифрованные с помощью EFS.

Таким образом, использование мандатного шифрования дает возможность реализовать криптографическую изоляцию информации в корпоративной сети:

1. Пользователям предоставляется возможность свободного использования съемного носителя в открытом режиме для любых целей вне корпоративной сети.

2. При работе внутри корпоративной сети, незашифрованные файлы, которые пользователь записал на съемный носитель вне данной сети, будут ему не доступны (кроме пользователей с явным разрешением).
3. При работе внутри корпоративной сети все файлы, записанные пользователем на съемные носители, будут зашифрованы в прозрачном режиме. Это снимает угрозу компрометации данных при утере (или краже) съемного носителя вне корпоративной сети.
4. Выбором политики используемых ключевых носителей для работы с EFS, администратор имеет также возможность минимизировать вероятность преднамеренной кражи информации с использованием съемных носителей. Один из подходов к решению данной проблемы состоит в хранении контейнера секретного ключа EFS непосредственно на компьютере корпоративной сети. Это обеспечивает невозможность для пользователя самостоятельного расшифрования файлов вне корпоративной сети.
5. Прозрачное использование EFS дает возможность пользователям корпоративной сети безопасно обмениваться зашифрованной информацией друг с другом посредством съемных носителей. Это реализуется благодаря возможности, предоставляемой EFS, которая позволяет явно задать список пользователей, которым будет дан криптографический доступ к зашифрованному файлу.

Список литературы

1. **Компания "КРИПТО-ПРО".** Формуляр. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 30 01.