Инструменты защиты информации локальной вычислительной сети

Белорусский государственный университет информатики и радиоэлектроники
г.Минск, Республика Беларусь

Ган-Ловкис В. С.
Зацепин Е.Н –канд. тех. наук, доцент

В данной статье рассмотрены возможные средства, применяемые для защиты информации локальной вычислительной сети.

Рассмотрим систему защиты информации «Панцирь для ОС Windows» с представлением соответствующих интерфейсов.

СЗИ включается в себя два приложения для работы пользователя: «Управление настройками»), и «Просмотрщик журналов аудита» (рисунок 1).

Данные программы используют в работе плагины (библиотеки четкой структуры). За редактирование и отображение настроек отвечают:

- subj_ctrlplg.dll - отображение и редактирование списка субъектов;
- prf_ctrlplg.dll - отображение и редактирование списка профилей;

За отображение событий зафиксированных механизмом управления доступом к файловой системе отвечает fc_logplg.dll.

Для обеспечения работы механизмов защиты была реализована служба armour_srv.exe, которая имеет плагин fc_srvplg.dll (загружает/запускает драйвер filectrl.sys, обслуживает некоторые запросы от этого драйвера).

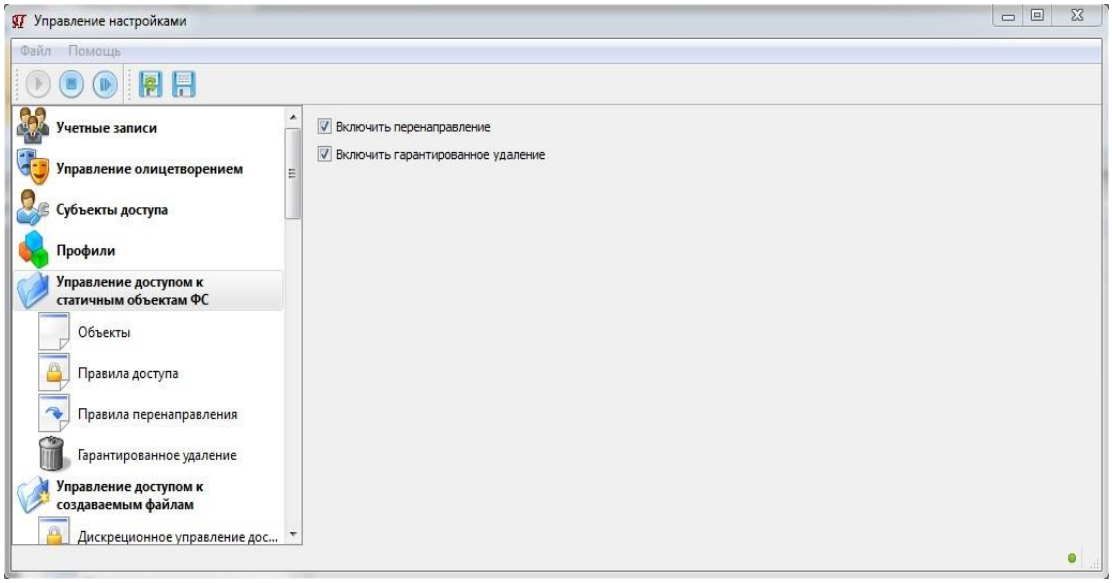

Рисунок 1 – Интерфейс «Управление настройками»

Общие библиотеки:

- fc_ctrlplg.dll - отображение и редактирование разграничений к файловой системе.
- armdrv.dll - предназначена для службы, чтобы драйвер armdrv.sys перечитывал настройки по различным событиям;

-armlpc.dll - предназначена для межпроцессного взаимодействия, а также для асинхронного взаимодействия драйвер-процесс;

-armsett.dll – содержит некоторые функции управления файлами настроек;

-rem*.dll - содержит диалоги обзора удаленных файловых систем.

Драйвера:

- armdrv.sys - общий драйвер, предназначен для поддержки других драйверов, управляет списком настроек (профили), списком работающих процессов, хранит журнал событий;
- filectrl.sys - реализует механизм разграничения прав доступа к файловой системе. Настройки берет в armdrv.sys, туда же записывает регистрируемые события. По архитектуре подобен минифильтрам.

Для настройки запустим интерфейс СЗИ: ctrliface.exe. Во вкладке «Субъекты доступа» создадим новый субъект доступа, в качестве субъектов доступа выступают пользователи системы и процессы. Субъект доступа задается тремя сущностями: эффективным и первичным пользователями и процессом. В данном случае не имеет значение, какой пользователь, и какой процесс инициирует действие над объектом доступа.

При создании будет задан вопрос о создании Профиля, на который следует ответить «да», после чего создастся новый Профиль «Любой», к которому будут относиться все разграничения, касающиеся пользователей, не обладающих административными правами. Профиль создается для удобства назначения для всех необходимых субъектов доступа одинаковых разграничений. Отдельно создадим субъект доступа «Администратор» для устранения отсутствия возможности устанавливать новое программное обеспечение или обновлять существующее. В субъекте доступа «Администратор» в качестве эффективного и первичного пользователя зададим пользователя с административными правами (Администратор), в качестве процессов зададим любой процесс (маска «*»)

«Администратор». Назначим исполнимые объекты доступа, которые являются исполняемыми.

Они имеют следующие расширения: *.com; *.exe; *.bat; *.cmd; *.vbs; *.vbe; *.js;*.jse; *.wsf; *.wsh и т.д. Назначим системные объекты доступа, которые необходимы для корректной работы операционной системы и необходимых программ. Они имеют расширения: *.config, *.dll,*.manifest, *.drv, *.fon, *.ttf, *.log, *.sys.

Системные и исполнимые объекты доступа будем назначать с учетом устранения недостатка, связанного с невозможностью разграничивать доступ к тем ресурсам, изменение которых мы не можем проконтролировать. Соответственно объект доступа будет задаваться в виде: «C:*.{расширение}».

Назначим информационные объекты доступа, как все остальные, кроме перечисленных объектов доступа, используя маску «*».

Для создания объекта доступа во вкладке «Управление доступом к статичным объектам ФС» → «Объекты» создадим все ОД с добавлением буквы системного диска.

Созданные объекты доступа представлены на рисунке.

После создания всех нужных объектов доступа, установим разграничения к ним. Представим реализуемую разграничительную политику:

Для создания разграничительной политики доступа используем вкладку «Управление доступом к статичным объектам ФС» → «Правила доступа». Выберем в выпадающем списке профиль, связанный с пользователем Администратор.

Теперь добавим новые правила согласно таблице для профиля «Все», связанного со всеми пользователями и процессами.

Создадим отдельный профиль для разграничения доступа для СЗИ и разрешим процессам, находящимся в папке «\ITB\Client» все: чтение, запись, исполнение, удаление, переименование.

Для защиты от утечки прав доступа и для устранения возможности повышения привилегий настроим механизм контроля олицетворения пользователей. Для этого используем вкладку «Управление олицетворением».

Запретим всем пользователям олицетворение с пользователем «Администратор».

Теперь реализуем в случае защиты от скриптовых деструктивных программ, субъекты доступа делятся на три типа:

- в качестве эффективного и первичного пользователя выступает Администратор с любым процессом;
- любой эффективный и первичный пользователь с любым процессом;

Объекты доступа также делятся на исполнимые, системные и информационные.

Реализуем разграничительную политику. Представим данные разграничения в виде таблицы прав доступа.

Для создания разграничительной политики доступа используем вкладку «Управление доступом к статичным объектам ФС» → «Правила доступа». В результате получим следующие разграничения:

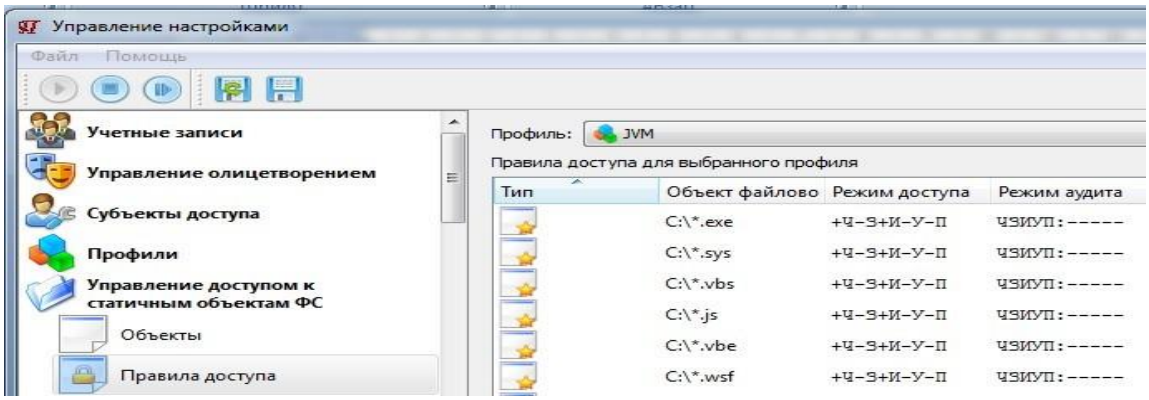

Рисунок 2 – Реализованная разграничительная политика

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Высокоскоростные ЛКС [Электронный ресурс]. – Электронные данные. – Режим доступа: http://citforum.ru.

[2] Кеннет, Г. Основы сетей Windows / Г. Кеннет. – М. : Диалектика 1999, – 237 с.

[3] Коммутаторы Ethernet. Начальные сведения [Электронный ресурс]. – Электронные данные. – Режим доступа: http://citforum.ru.