

Лабораторная работа 9. Мандатный механизм разграничения доступа к файловым объектам

Цель лабораторной работы: практическое изучение мандатного механизма разграничения доступа на основе программного продукта Secret Net 5.1 (автономный вариант).

Задачи лабораторной работы:

1. Настройка категорий конфиденциальности
2. Настройка субъектов доступа
3. Настройка объектов доступа (данные)
4. Контроль потоков данных

Задание

Контрольные вопросы

Содержание лабораторной работы:

1. Настройка категорий конфиденциальности

Доступ пользователя к информации, содержащейся в конфиденциальном файле, осуществляется при условии, если пользователю назначен соответствующий уровень допуска. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов.

Запустите «Локальные параметры безопасности» под учетной записью «Администратор»: «Пуск - Все программы - Secret Net 5 - Локальная политика безопасности», перейдите в группу «Параметры Secret Net 5 Настройка подсистем - настройка подсистем».

Параметр «Полномочное управление доступом: название уровней конфиденциальности» настройте, как показано на рис. 1.

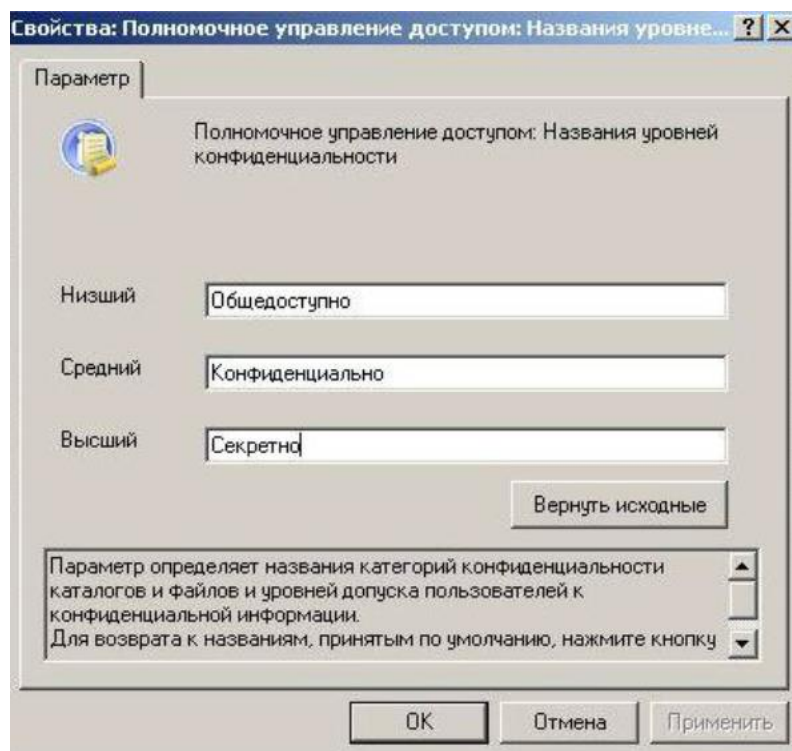


Рис. 1 - Параметр «Название уровней конфиденциальности»

2. Настройка субъектов доступа

Запустите «Управление компьютером» под учётной записью «Администратор»: «Пуск - Все программы - Secret Net 5 - Управление компьютером», перейдите в группу «Локальные пользователи и группы - Пользователи».

Далее настройте права администратора. Для этого в свойствах учётной записи «Администратор» перейдите на вкладку Secret Net 5. В группе «Доступ» установите следующие значения (рис. 2).

Рис. 2 - Настройка прав доступа пользователя «Администратор»

- *Управление категориями конфиденциальности* - пользователь может изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска; управлять режимом наследования категорий конфиденциальности каталогов.
- *Печать конфиденциальных документов* - используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном режиме контроля печати конфиденциальных документов.
- *Вывод конфиденциальной информации* - пользователю разрешается выводить конфиденциальную информацию на внешние носители.

После чего вернитесь в оснастку «Локальные пользователи и группы – Пользователи». Создайте пользователя, выбрав «Новый пользователь» в контекстном меню или в меню «Действие». Настройте учётную запись как показано на рис. 3 и нажмите кнопку «Создать».

Рис. 3 - Создание пользователя

По аналогии создайте пользователя «Секретный».

Для настройки прав доступа перейдите в группу «Пользователи», выделите пользователя «Конфиденциальный». В контекстном меню выберите «Свойства». В группе «Доступ» настройте параметры как показано на рис. 4, предоставив право вывода информации на внешние носители и печать конфиденциальных документов.

Для пользователя «Секретный» выберите уровень допуска «Секретно», запретив вывод на внешние носители и печать конфиденциальных документов (рис. 5).

Для применения настроек завершите сеанс и повторно войдите под учётной записью «Администратор».

Рис. 4 - Настройка прав доступа пользователя «Конфиденциальный»

Рис. 5 - Настройка прав доступа пользователя «Секретный»

3. Настройка объектов доступа (данные)

В механизме полномочного управления доступом используются следующие категории конфиденциальности:

- *неконфиденциально (в нашем случае «общедоступно»);*
- *конфиденциально;*

- *строго конфиденциально (в нашем случае «секретно»).*

Категория конфиденциальности относится к атрибутам ресурса (каталога или файла). Повышение категорий конфиденциальности нужных ресурсов осуществляется пользователями в пределах своих уровней допуска. В механизме полномочного управления доступом используется принцип наследования файлами категории конфиденциальности каталога.

Присвоение новым файлам категории конфиденциальности каталога может выполняться автоматически или по запросу. Включение и отключение режима автоматического присвоения категории осуществляется в диалоговом окне настройки свойств каталога (параметр «Автоматически присваивать новым файлам», рис. 6).

Рис. 6 - Выбор категории конфиденциальности ресурса

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию «Управление категориями конфиденциальности». Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS.

Для изменения категории конфиденциальности каталога или файла в режиме мандатного разграничения доступа необходимо обладать привилегией «Управление категориями конфиденциальности». Если у пользователя нет такой привилегии, то он может только повысить категорию конфиденциальности файла, но не выше своего уровня допуска или уровня конфиденциальности сеанса.

В проводнике вызовите контекстное меню каталога «D:\temp» и выберите «Свойства». В окне «Свойства» откройте вкладку «Secret Net» (рис. 6).

Укажите для каталога следующие значения параметров:

- *выберите в раскрывающемся списке поля «Категория» категорию «Конфиденциально»;*
- *установите режим автоматического присвоения категории конфиденциальности файлам каталога, включив параметр «Автоматически присваивать новым файлам».*

Нажмите кнопку «ОК».

Если каталог содержит файлы и подкаталоги, на экране появится диалоговое окно, предлагающее изменить категории конфиденциальности вложенным файлам и каталогам (рис. 7).

Рис. 7 - Изменение категории конфиденциальности вложенных каталогов и файлов

Изменение категории конфиденциальности файла производится аналогично.

Пользователю разрешается доступ к файлу, если уровень допуска пользователя не ниже категории конфиденциальности файла. Например, пользователю с уровнем допуска «Конфиденциально» разрешается выполнять чтение файлов с категориями «Конфиденциально» и «Общедоступно», но запрещено открывать файлы с категорией «Секретно». Уровень допуска «Секретно» предоставляет возможность открывать файлы с любой категорией конфиденциальности.

Если категория допуска пользователя выше, чем метка конфиденциальности каталога с документами, то пользователь может открывать документы, но изменять и сохранять в этой же папке не сможет, также запрещено создавать и удалять документы в папках, категория конфиденциальности которых меньше категории допуска пользователя.

Войдите под учётной записью «user» (уровень допуска «Общедоступно»). Попробуйте открыть файл «D:\temp\Конф.txt». Операционная система выдаст ошибку

доступа к этому файлу (рис. 8). Попробуйте удалить этот файл. Операционная система выдаст ошибку удаления этого файла (рис. 9). Попробуйте скопировать файл в общедоступный каталог (например, «Рабочий стол»). Операционная система выдаст ошибку копирования файла (рис. 10). Попробуйте создать новый файл в каталоге «test». Операционная система выдаст ошибку создания файла (рис. 11).

Таким образом, под учётной записью с уровнем допуска «Общедоступно» запрещены любые действия с файловыми объектами уровня «Конфиденциально» (пользователь не может работать с документами, чья категория конфиденциальности выше его уровня допуска).

Рис. 8 - Ошибка доступа к конфиденциальному файлу

Рис. 9 - Ошибка удаления конфиденциального файла

Рис. 10 - Ошибка копирования конфиденциального файла

Рис. 11 - Ошибка создания файла в конфиденциальном каталоге

Войдите под учётной записью «Секретный». Попробуйте открыть файл «D:\temp\Конф.txt» - будет выдано окно с предложением о повышении уровня конфиденциальности приложения (рис. 12). Работа с файлом будет разрешена только после повышения уровня. Скопируйте файл в общедоступный каталог (например, «Рабочий стол»). Посмотрите уровень конфиденциальности у скопированного файла. После копирования был присвоен уровень «Общедоступно». Попробуйте скопировать данные из файла «D:\temp\Конф.txt» в любой файл с меткой «Общедоступно». Уровень конфиденциальности у общедоступного файла не изменился.

Рис. 12 - Повышение уровня конфиденциальности приложения

Таким образом, возможность копирования конфиденциальных файлов в общедоступный каталог или самих конфиденциальных данных в общедоступный файл может привести к утечке информации. При таком подходе ответственность за конфиденциальность информации лежит на пользователях, которым разрешён доступ к информации.

4. Контроль потоков данных

4.1. Включение контроля потоков данных

Запретить пользователям возможность понижения уровня конфиденциальности информации можно при помощи контроля потоков данных.

Войдите под учётной записью «Администратор». Запустите «Локальные параметры безопасности»: «Пуск - Все программы - Secret Net 5 - Локальная политика безопасности», перейдите в группу «Параметры Secret Net - Настройки подсистем». Выберите параметр «Полномочное управление доступом: Режим работы» и включите контроль потоков.

Рис. 13 - Включение контроля потоков данных

4.2. Работа с конфиденциальными файлами при более высоком уровне сеанса

Перезагрузите операционную систему для применения настроек и войдите под учётной записью «Секретный». При входе появляется предложение выбрать уровень сеанса, определяющего, с каким уровнем конфиденциальности файлов будет проходить работа (рис. 14). Выберите уровень сеанса «Секретно».

Рис. 14 - Выбор уровня конфиденциальности сеанса

Откройте файл «D:\temp\Конф.txt». Попробуйте удалить этот файл, изменить и сохранить его, скопировать в общедоступный каталог (например, «Рабочий стол»). Попробуйте создать новый файл в каталоге «test». Таким образом, если включен контроль потоков данных, то при уровне сеанса более высоком, чем уровень конфиденциальности файла, все действия, кроме чтения, запрещены.

Измените файл «D:\temp\Конф.txt» и попробуйте его сохранить под другим именем или в другой каталог. Сохранение будет невозможно (рис. 15), т.к. уровень сеанса выше, чем уровень конфиденциальности каталогов.

Рис. 15 - Ошибка сохранения информации при контроле потоков в каталог с меньшим уровнем конфиденциальности, чем уровень сеанса

4.3. Работа с конфиденциальными файлами при равном уровне сеанса

Войдите под учётной записью «Секретный» и выберите уровень сеанса «Конфиденциально».

Откройте файл «D:\temp\Конф.txt». Измените и сохраните этот файл, создайте новый файл в каталоге «test». Попробуйте скопировать его в общедоступный каталог (например, «Рабочий стол»).

Скопируйте текст из файла «Конф.txt» в файл «Общее.txt» и попробуйте сохранить файл «Общее.txt». Произойдёт отказ в доступе из-за попытки понизить уровень конфиденциальности информации. Сохраните файл «Общее.txt» в конфиденциальный каталог «test».

Измените какую-либо настройку операционной системы (например, отображение вкладки «Безопасность»: измените параметр «Использовать простой общий доступ к файлам» в разделе «Панель управления - Свойства папки»). Перезапустите вкладку «Свойства папки» и проверьте состояние параметра. Попробуйте запустить «Outlook». Изменения настроек операционной системы и приложений записываются в общедоступные файлы, поэтому их сохранение не происходит.

Таким образом, если включен контроль потоков данных, то при уровне сеанса, равном уровню конфиденциальности файла, все действия разрешены, кроме копирования информации в файлы с более низким уровнем конфиденциальности.

Попробуйте скопировать файл «D:\temp\Конф.txt» на сменный носитель. Копирование не удастся, т.к. данному пользователю не было представлено право копирования конфиденциальной информации на сменный носитель.

4.4. Работа при уровне сеанса «Общедоступно»

Войдите под учётной записью «Секретный» и выберите уровень сеанса «Общедоступно».

Попробуйте открыть, удалить файл «D:\temp\Конф.txt», скопировать его в общедоступный каталог (например, «Рабочий стол») и на сменный носитель. При уровне

сеанса «Общедоступно» любой доступ к конфиденциальной информации запрещён. В то же время доступ к общедоступной информации неограничен: запустите «Outlook», скопируйте общедоступный файл на сменный носитель.

Таким образом, за счёт подхода, основанного на контроле потоков данных, исключается возможность утечки конфиденциальной информации.

4.5. Копирование конфиденциальных файлов на сменный носитель

Войдите под учётной записью «Конфиденциальный». При первом входе необходимо настроить операционную систему, что возможно только при сеансе «Общедоступно», поэтому доступ к конфиденциальной информации запрещён (рис. 16).

Завершите сеанс и снова войдите под учётной записью «Конфиденциальный», выбрав уровень сеанса «Конфиденциально».

Скопируйте файл «D:\temp\Конф.txt» на сменный носитель. При копировании появится предупреждение о потере файлом уровня конфиденциальности (рис. 17). Несмотря на потерю конфиденциальности, копирование будет разрешено, т.к. пользователю было предоставлено право вывода конфиденциальной информации на сменные носители (рис. 4).

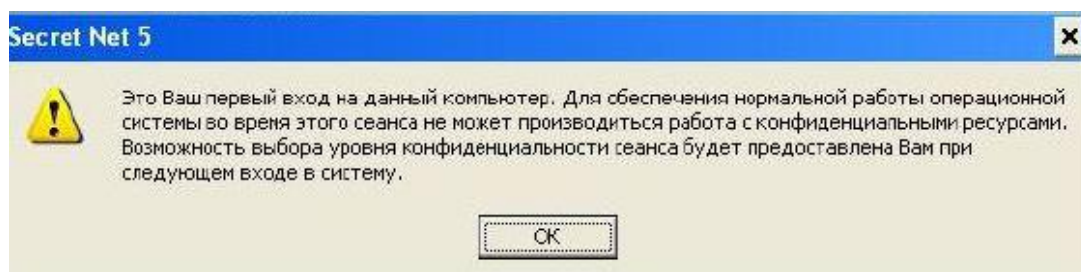


Рис. 16 - Первый вход в операционную систему

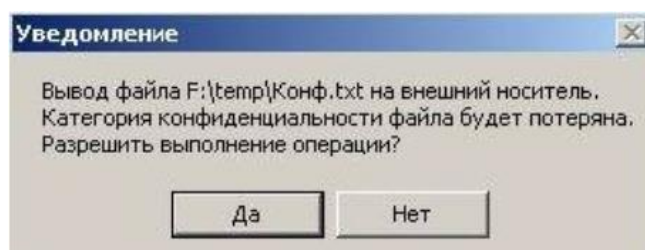


Рис. 17 - Предупреждение о потере файлом конфиденциальности при копировании на сменный носитель

Задание

1. В соответствии с табл. 1 от имени администратора присвойте каталогам (находящимся в корне диска D:\) категории конфиденциальности.
2. В каждом каталоге создайте 2-4 документа от имени пользователя, допуск которого соответствует категории конфиденциальности каталога.
3. Проверьте возможность доступа к созданным документам.

Таблица 1. Варианты заданий

Вариант	Каталог и его категория конфиденциальности		
	доступно	конфиденциально	секретно
1	Б:\БД\Заказы	Б:\БД\Поставщики	Б:\БД\Клиенты
2	Б:\Договоры\Спонсоры	Б:\Договоры\Инвесторы	Б:\Договоры\Партнёры
3	D:\Документация\Отчёты	D:\Документация\Приёмные документы	D:\Документация\Информация о сотрудниках
4	D:\Подразделения\Отдел	D:\Подразделения\Отдел	D:\Подразделения\Фина

	сбыта	кадров	нсовый отдел
5	D:\Файлы\Пользователи	D:\Файлы\Опытные пользователи	D:\Файлы\Администраторы
6	D:\Поставщики	D:\БД\Заказы	D:\БД\Клиенты
7	D:\Договоры\Партнёры	D:\Договоры\Спонсоры	D:\Договоры\Инвесторы
8	D:\Подразделения\Отдел кадров	D:\Подразделения\Финансовый отдел	D:\Подразделения\Отдел сбыта
9	D:\Файлы\Опытные пользователи	D:\Файлы\Пользователи	D:\Файлы\Администраторы
10	D:\Документация\Приёмные документы	D:\Документация\Отчёты	D:\Документация\Информация о сотрудниках

Контрольные вопросы

1. На чём основан принцип действия мандатного механизма разграничения доступа?
2. Разрешается ли пользователю доступ к файлу, если уровень допуска пользователя выше категории конфиденциальности файла?
3. Что означает функция «Вывод конфиденциальной информации»?
4. Перечислите категории конфиденциальности по умолчанию.
5. Какой параметр предоставляет возможность управлять категориями конфиденциальности?
6. Можно ли присвоить категорию конфиденциальности ресурсу, расположенному на диске с файловой системой FAT32?
7. Поясните параметр «Автоматически присваивать новым файлам».
8. Для чего нужен контроль потоков данных?
9. При каком уровне сеанса пользователь может изменять настройки операционной системы и приложений?
10. Какие права предоставляются пользователю при доступе к конфиденциальной информации, уровень которой ниже уровня сеанса?

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях