**Практическая работа 16**

**Настройка политики безопасности**

***Цель работы:*** ознакомиться с методами ограничения доступа к информации

***Теоретическая часть***

Разграничение доступа является достаточно эффективным средством предупреждения возможного ущерба вследствие нарушения целостности или конфиденциальности информации. В том случае, если доступ к самому компьютеру или к его ресурсам может получить пользователь, который имеет злой умысел или недостаточный уровень подготовки, он может случайно или преднамеренно исказить информацию или уничтожить ее полностью или частично.

Это же обстоятельство может привести к раскрытию закрытой информации или несанкционированному тиражированию открытой, например, программ, баз данных, разного рода документации, литературных произведений и т. д. в нарушение прав собственников информации, авторских прав…

С точки зрения разграничения доступа, в информационных системах следует различать *субъекты доступа и объекты доступа*. В число *субъектов доступа* могут войти либо персонал информационной системы, либо посторонние лица. *Объектами доступа* являются аппаратно-программные элементы информационных систем. Чаще всего в качестве объектов доступа рассматриваются файлы (в том числе папки и файлы программ). Доступ к объекту может рассматриваться либо как чтение (получение информации из него), либо как изменение (запись информации в него). Тогда виды доступа определяются следующими возможными сочетаниями этих операций:

• ни чтение, ни изменение;

• только чтение;

• только изменение;

• и чтение, и изменение.

Очевидно, что различие функциональных обязанностей субъектов обусловливает необходимость предоставления им соответствующих видов доступа.

Управление доступом пользователей и глобальными параметрами на членах домена осуществляется на двух уровнях: локальной системы и домена. На отдельных компьютерах доступ пользователей конфигурируют на уровне локальной системы, а одновременно для нескольких систем или ресурсов, входящих в домен, — на уровне домена.

Права доступа пользователя определяются руководителем организации и прописываются на рабочей станции системным администратором (администратором домена).

Процедура проверки прав доступа включает авторизацию и аутентификацию. Авторизация предполагает проверку уровня доступа к объекту, а аутентификация — проверку подлинности пользователя. Для аутентификации обычно используются имя пользователя (login) и пароль (password). Системный администратор осуществляет разграничение прав доступа в соответствии с заданной системной политикой, которая предполагает:

• ограничения на минимальную длину, сложность и срок действия пароля;

• требование уникальности паролей;

• блокировку пользователя при неудачной аутентификации;

• ограничение времени и места работы пользователя.

***Система разграничения доступа реализована*** так, что при повседневной работе пользователи не должны замечать, что любое обращение к любому объекту проходит проверку на соответствие установленным правам доступа. Списки прав доступа можно задавать на каждый документ отдельно. При создании документа автоматически задается такой доступ на него, чтобы создатель имел все права.

***Система разграничения доступа предназначена*** для реализации определенных администратором защиты правил на выполнение операций пользователями над объектами хранилища.

Система ограничения прав доступа не может дать полной гарантии безопасности информации. Дело в том, что злоумышленник может получить или подобрать пароль легального пользователя. Кроме того, опытный специалист может обойти систему разграничения доступа. Средством обнаружения несанкционированного доступа к ресурсам служат системы аудита, которые автоматически фиксируют доступ к файлам и папкам и системные события.

**Модели разграничения доступа**

Наиболее распространенные модели разграничения доступа:

* *дискреционная* (избирательная) модель разграничения доступа;
* полномочная (*мандатная*) модель разграничения доступа.

**Дискреционная модель** характеризуется следующими правилами:

* любой объект имеет владельца;
* владелец имеет право произвольно ограничивать доступ субъектов к данному объекту;
* для каждого набора субъект – объект – метод право на доступ определен однозначно;
* наличие хотя бы одного привилегированного пользователя (например, администратора), который имеет возможность обращаться к любому объекту с помощью любого метода доступа.

В дискреционной модели определение прав доступа хранится в матрице доступа: в строках перечислены субъекты, а в столбцах – объекты. В каждой ячейке матрицы хранятся права доступа данного субъекта к данному объекту.



**Полномочная модель** характеризуется следующими правилами:

* каждый объект обладает грифом секретности. Гриф секретности имеет числовое значение: чем оно больше, тем выше секретность объекта;
* у каждого субъекта доступа есть уровень допуска. Допуск к объекту в этой модели субъект получает только в случае, когда у субъекта значение уровня допуска не меньше значения грифа секретности объекта.

Преимущество полномочной модели состоит в отсутствии необходимости хранения больших объемов информации о разграничении доступа. Каждым субъектом выполняется хранение лишь значения своего уровня доступа, а каждым объектом – значения своего грифа секретности.

***Методы разграничения доступа***

*Виды методов разграничения доступа:*

 1.**Разграничение доступа по спискам**

 Суть метода состоит в задании соответствий: для каждого пользователя задается список ресурсов и права доступа к ним или для каждого ресурса определяется список пользователей и права доступа к этим ресурсам. С помощью списков возможно установление прав с точностью до каждого пользователя. Возможен вариант добавления прав или явного запрета доступа. Метод доступа по спискам используется в подсистемах безопасности операционных систем и систем управления базами данных.

2. **Использование матрицы установления полномочий**

При использовании матрицы установления полномочий применяется матрица доступа (таблица полномочий). В матрице доступа в строках записываются идентификаторы субъектов, которые имеют доступ в компьютерную систему, а в столбцах – объекты (ресурсы) компьютерной системы. В каждой ячейке матрицы может содержаться имя и размер ресурса, право доступа (чтение, запись и др.), ссылка на другую информационную структуру, которая уточняет права доступа, ссылка на программу, которая управляет правами доступа и др. Данный метод является достаточно удобным, так как вся информация о полномочиях сохраняется в единой таблице. Недостаток матрицы – ее возможная громоздкость.

3. **Разграничение доступа по уровням секретности и категориям**

Разграничение по степени секретности разделяется на несколько уровней. Полномочия каждого пользователя могут быть заданы в соответствии с максимальным уровнем секретности, к которому он допущен. При разграничении по категориям задается и контролируется ранг категории пользователей. Таким образом, все ресурсы компьютерной системы разделены по уровням важности, причем каждому уровню соответствует категория пользователей.

4. **Парольное разграничение доступа**

Парольное разграничение использует методы доступа субъектов к объектам с помощью пароля. Постоянное использование паролей приводит к неудобствам для пользователей и временным задержкам. По этой причине методы парольного разграничения используются в исключительных ситуациях.

На практике принято сочетать разные методы разграничений доступа. Например, первые три метода усиливаются парольной защитой. Использование разграничения прав доступа является обязательным условием защищенной информационной системы.

***Практическая часть*** – можно ничего не менять в своих настройках. Просто прогуляйтесь по указанным путям и сделайте соответствующие скрин-шоты.

1. *Освоить средства разграничения доступа пользователей к папкам*:
* выполнить команду «Общий доступ и безопасность» контекстного меню папки (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»;
* открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;
* с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);
* включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;
* открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;
* открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;



* закрыть окно дополнительных параметров безопасности.

2. *Освоить средства разграничения доступа пользователей к файлам*:

* выполнить команду «Свойства» контекстного меню файла;
* повторить все задания п. 1, но применительно не к папке, а к файлу.

3. *Освоить средства разграничения доступа к принтерам*:

* выполнить команду «Принтеры и факсы» меню «Пуск»;
* выполнить команду «Свойства» контекстного меню установленного в системе принтера;
* повторить все задания п. 1, но применительно не к папке, а к принтеру.

4. *Освоить средства разграничения доступа к разделам реестра операционной системы*:

* с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);
* с помощью команды «Разрешения» меню «Правка» редактора реестра определить сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита;
* включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце.

**Так как версии операционных систем у всех разные, то возможны отклонения от указанных маршрутов. Придется догадываться самим ))** 

Отчет должен содержать:

1. Тему и цель работы
2. Экранные копии выполнения работы
3. Составьте матрицу доступа по своей (курсовой) ИС.
4. Ответы на контрольные вопросы.

***Контрольные вопросы***:

1. В чем достоинства дискреционной политики безопасности?
2. В чем недостатки мандатной политики безопасности?
3. Кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
4. В чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам?
5. В чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам?
6. В чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам?