НАСТРОЙКА ПРАВ ДОСТУПА К ФАЙЛАМ В ОС WINDOWS SERVER 2016

SETTING UP RIGHT ACCESS TO FILES FOR WINDOWS SERVER 2016

УДК 004.451

Дворников Сергей Викторович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Dvornikov S.V. sergey.dv520@gmail.com

Аннотация

Важно контролировать какие данные может читать или выполнять тот или иной пользователь в сети. Для управления правами доступа к файлам используют списки контроля доступа в операционной системе Windows Server 2016. В данной работе показаны теоретические и практические аспекты настройки списков контроля доступа.

Annotation

It is important to control what data can be read or performed by a particular user on the network. Access control lists in the Windows Server 2016 operating system are used to manage access rights to files. This paper shows the theoretical and practical aspects of configuring access control lists.

Ключевые слова: защита информации, права доступа, идентификатор, разрешение.

Key words: information security, access rights, ID, permission.

Тема данной работы связана с решением проблемы защиты информации в корпоративных сетях. Любая организация, в которой более нескольких

компьютеров использует ЛВС. И в каждой ЛВС в той или иной степени необходимо защищать информацию.

Подтверждениями актуальности данной работы можно привести примеры из отчета, проведенного компанией Infowatch [1]. Данные из аналитического отчета:

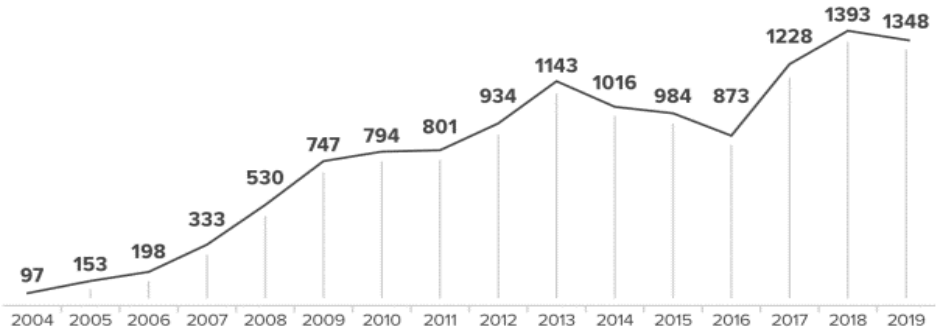


Рисунок 1 – График утечек информации.



Рисунок 2 – Диаграммы утечек информации по правам пользователей.

Из графика видно (рис. 1), что тенденция утечек информации увеличивается с годами, а по диаграммам видно (рис. 2), что это происходит в большей степени по причине обычных сотрудников.

Исходя из вышесказанного повышение защиты информации в корпоративных сетях встроенными средствами Windows Server 2016.

Для определения иерархии хранения данных на диске используется файловая система. В ОС Windows по умолчанию для несъемных дисков используется файловая система NTFS. Для разграничения доступа к файлам и папкам в файловой системе NTFS используют список контроля доступа или Access Control List (ACL) [2]. Каждому объекту задается свой ACL, где выбираются разрешения для пользователей или групп. Назначать права можно двумя способами: первый с помощью проводника и вкладки Безопасность, второй

– с помощью утилиты icacls.exe. Настройка прав доступа к объектам реализуется с помощью записей в таблице Master File Table (MFT). Каждому файлу соответствует запись в таблице MFT. В каждой записи хранится два списка контроля доступа:

1) Системный список управления доступом (SACL). Применяется для фиксирования попыток доступа к объектам.

2) Список управления избирательным доступом (DACL). В нем и определяется у кого есть доступ, а у кого нет.

В каждом ACL есть набор записей контроля доступа - Access Control Entries (ACE).

Записи ACE бывают разрешающие доступ и запрещающие доступ. Каждая запись содержит три поля:

1) SID пользователя или группы к кому применяется правило доступа.

2) Вид доступа, на которое распространяется правило.

3) Запрещающий или разрешающий тип ACE.

SID (Security Identifier) – уникальный идентификатор, который присваивается в момент создания каждому пользователю или группе пользователей. Используется для идентификации учетной записи, группы, службы или домена в сети. По SID применяются политики безопасности. Например, в случае изменении имени пользователя права доступа у него остаются такие же. SID использует «машина», а имя пользователя или группы для пользователей.

Если в записи у какого-либо объекта отсутствует список управления избирательным доступом, то к объекту есть доступ для всех. Если в списке управления избирательным доступом отсутствует ACE – доступа к файлу нет ни у кого. Разрешения для файлов и папок отличаются.

Разрешения для папок также определяют разрешения и для вложенных в них папок и файлов. В «Группы или пользователи» - это SID [3], только в читабельном виде. Чтобы узнать полный SID как он используется в системе необходимо обратиться к командной строке либо к реестру. Разрешения для группы «Система» - это ACL (рис. 3).

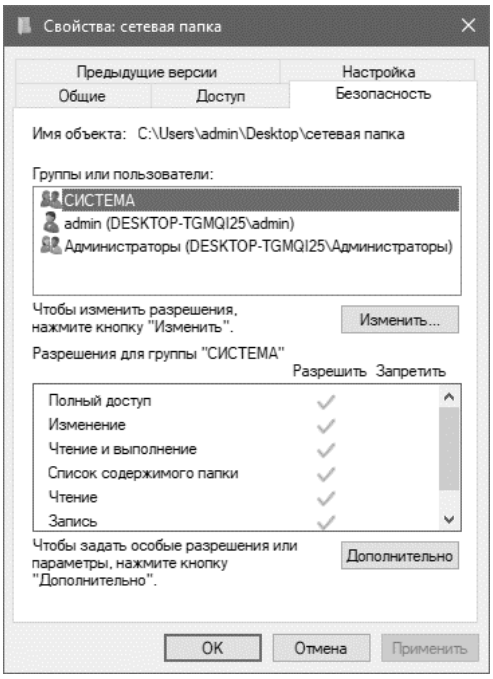


Рисунок 3 – Разрешения для папок.

SID можно узнать введя в командную строку (cmd) команду «wmic useraccount where name=’user’ get sid» [4] в командную строку. Где ’user’ – имя учетной записи. Ответом будет строка типа: S-1-5-21-3344360940-2582655908-2518626230-1002. Также можно узнать SID всех пользователей компьютера введя команду «wmic useraccount list full».

Рассмотрим разрешения для папок и файлов подробнее (таблица 1). [5]

Таблица 1 – Разрешения для папок и файлов.

Разрешение	Разрешаемые действия для папок	Разрешаемые действия для файлов
Полный доступ	Все нижеперечисленные разрешения, кроме особых	
Изменение	Разрешает действия, которые включают разрешения «Чтение» и «Чтение и выполнение»	Позволяет чтение, запись, удаление файлов.
Чтение и выполнение	Разрешает доступ к вложенным файлам, если нет доступа к данной папке.	Разрешает просмотр и запуск исполняемых файлов.
Список содержимого папки	Разрешает видеть вложенные файлы и папки.	

Чтение	Позволяет видеть вложенные файлы и папки и их атрибуты.	Доступ и просмотр файлов.
Запись	Позволяет создавать вложенные файлы и папки.	Запись данных в файл.
Особые разрешения	Настраиваются индивидуально, используя дополнительные настройки.	

Данные базовые (стандартные) разрешения созданы путем соединения особых разрешений (таблица 2). [6]

Таблица 2 – Особые разрешения для папок.

Особые разрешения	Полный доступ	Изменить	Чтение и выполнение	Список содержимого папки	Чтение	Запись
Обзор папок	•	•	•	•		
Содержание папки	•	•	•	•	•	
Чтение атрибутов	•	•	•	•	•	
Чтение дополнительных атрибутов	•	•	•	•	•	
Создание файлов	•	•				•
Создание папок	•	•				•

Атрибуты файлов описывают свойства файла или папки.

Выделяют четыре основных атрибута для файлов:

1) Только для чтения – запрещает изменение файлов и папок
2) Скрытый – скрывает файлы и папки.
3) Системный – используется для системных файлов.
4) Архивный – используется программами для резервного копирования.

Также есть атрибуты, которые появились в более новых версиях Windows такие как сжатия, шифрования, индексирования, времени, атрибут целостности, без очистки. Некоторые из них можно посмотреть в дополнительных атрибутах (рис. 4).

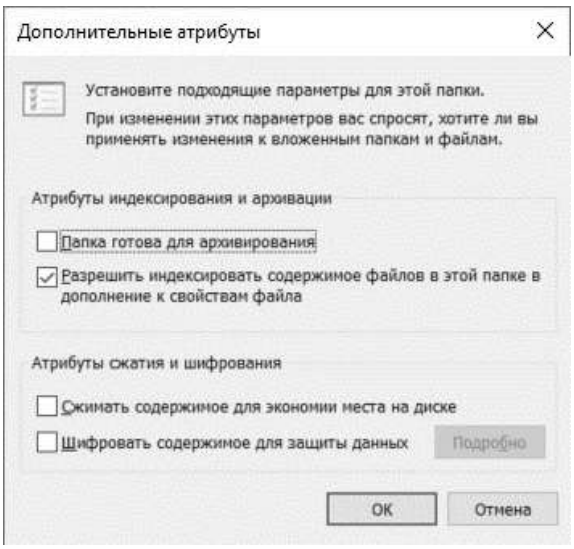


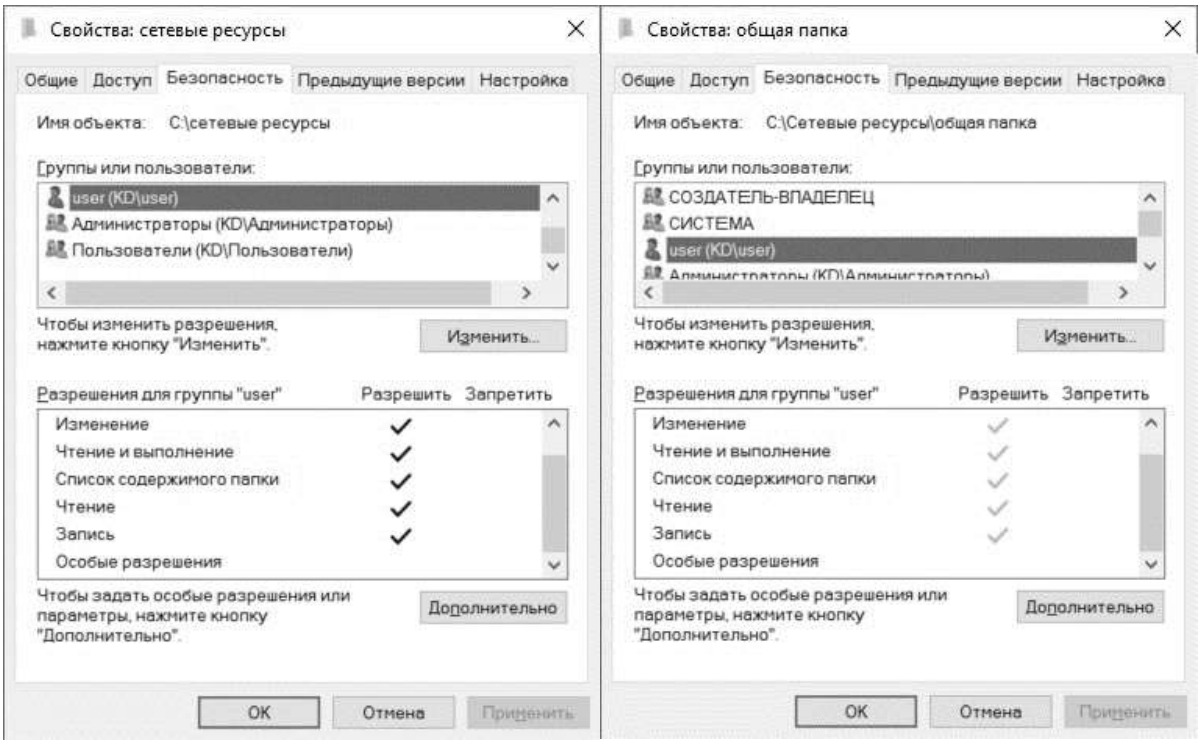
Рисунок 4 – Дополнительные атрибуты

Настраивая права доступа к папкам и файлам нужно учитывать наследование прав. Наследование – это применение прав доступа к вложенным папкам и файлам от папки, к которой были применены права доступа.

Рассмотрим пример назначения прав доступа и наследования:

Для папки «Сетевые ресурсы» в «группы или пользователи» добавим пользователя user и назначим ему полные права. Права, которые мы можем изменить или добавить к существующим выделены «галочками» темного цвета (рис. 5а). На следующем рисунке (рис. 5б) видно, что «галки» стали бледнее, это означает, что права данной папки унаследованы от папки старшей «Сетевые ресурсы».

Все разрешения, которые наследуются называются неявными. Права доступа, которые выставляются вручную называются явными. Отсюда можно выделить два пункта. Первый – запрещающее разрешение права доступа, применяемые к одному SID на одном уровне, имеет более высокий приоритет чем разрешающее. Второй – явное разрешение имеет более высокий приоритет, чем неявное. Явное разрешение приоритетнее неявного.



а) б)

Рисунок 5 – Свойства папки «сетевые ресурсы» и вложенной «общей папки»

При копировании объекта с одного логического диска на другой, копируемый объект получает права того каталога куда он копируется.

При перемещении объекта в пределах одного логического диска, объект сохраняет свои разрешения, меняется только запись в таблице MFT.

При копировании объекта в пределах одного логического диска, объект получает разрешения от вышестоящего объекта.

Сетевые разрешения не зависят от типа файловой системы и применяются только для доступа к сетевым файлам. К локально авторизованному пользователю сетевые разрешения не буду применятся. Также в случае если данные располагаются в файловой системе FAT, то локально авторизованному пользователю будет доступен полный доступ к этим данным, если данные в файловой системе NTFS, то права доступа будут определяться данной файловой системой.

Таким образом были рассмотрены права доступа в операционной системе Windows. Теоретические и практические материалы данной работы позволят выполнить настройку контроля доступа в реальных задачах и обезопасить необходимые данные от ненужных просмотров.

Литература

1. Infowatch.ru – [Электронный ресурс]. – Режим доступа – URL: https://www.infowatch.ru/
2. Заметки о Windows «Настройка разрешений файловой системы NTFS» – [Электронный ресурс]. – Режим доступа: https://windowsnotes.ru/other/nastrojka-razreshenij-fajlovoj-sistemy-ntfs/
3. Ripplefaq.ru «Разрешения для файла определяются используемой. Настройка прав для файлов и папок» – [Электронный ресурс]. – Режим доступа: https://ripplefaq.ru/wipe-android/razresheniya-dlya-faila-opredelyayutsya-ispolzuemoi-nastroika-prav-dlya-failov-i.html
4. Pyatilistnik.org «Как узнать sid пользователя windows в домене» – [Электронный ресурс]. – Режим доступа: http://pyatilistnik.org/kak-uznat-sid-polzovatelya-windows-v-domene/
5. Студопедия «Права доступа, наследование прав доступа, взятие во владение, аудит доступа к ресурсам» – [Электронный ресурс]. – Режим доступа: https://studopedia.ru/14_128776_prava-dostupa-nasledovanie-prav-dostupa-vzyatie-vo-vladenie-audit-dostupa-k-resursam.html
6. Studfile.net «Особые разрешения для файлов и папок» – [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/5368379/page:9/

Literature

1. Infowatch.ru - [Electronic resource]. - Access mode - URL: https://www.infowatch.ru/
2. Notes about Windows "Setting permissions of the NTFS file system" - [Electronic resource]. - Access mode: https://windowsnotes.ru/other/nastrojka-razreshenij-fajlovoj-sistemy-ntfs/
3. Ripplefaq.ru “Permissions for the file are determined by the file used. Setting rights for files and folders”- [Electronic resource]. - Access mode: https://ripplefaq.ru/wipe-android/razresheniya-dlya-faila-opredelyayutsya-ispolzuemoi-nastroika-prav-dlya-failov-i.html

4. Pyatilistnik.org "How to find out the sid of a windows user in a domain" - [Electronic resource]. - Access mode: http://pyatilistnik.org/kak-uznat-sid-polzovatelya-windows-v-domene/
5. Studopedia "Access rights, inheritance of access rights, takeover, audit of access to resources" - [Electronic resource]. - Access mode: https://studopedia.ru/14_128776_prava-dostupa-nasledovanie-prav-dostupa-vzyatie-vo-vladenie-audit-dostupa-k-resursam.html
6. Studfile.net "Special permissions for files and folders" - [Electronic resource]. - Access mode: https://studfile.net/preview/5368379/page:9/