МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Теория

по лабораторной работе №2

«Администрирование и управление ресурсами Windows Server»

по дисциплине

«Программное обеспечение вычислительных сетей»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Кочешков А. А.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Сухоруков В.А.\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_19-В-2\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2022

# Понятия объекта безопасности и субъекта безопасности. Состав и идентификация субъектов безопасности конкретного компьютера в домене. Специфика встроенных (предустановленных) субъектов.

Субъект безопасности - это любая сущность, которая может быть проверена службой операционной системы, например учетная запись пользователя, учетная запись компьютера или поток или процесс, который выполняется в контексте безопасности пользователя, учетная запись компьютера или группы безопасности для этих учетных записей. Субъекты безопасности являются основой для управления доступом к защищаемым ресурсам на компьютерах с Windows. Каждому субъекту безопасности представлен уникальный идентификатор безопасности (SID) в операционной системе.

Субъекты безопасности выполняют действия (включая чтение, запись, изменение или полный доступ) над объектами.

В системе Windows имеется множество типов объектов безопасности. Для каждого типа есть свой менеджер и свои функции, поэтому для каждого типа определен свой набор разрешений. Основными типами объектов с точки зрения управления безопасностью являются следующие:

* Объекты файловой системы NTFS – файлы и каталоги (чтение, чтение и выполнение, запись, изменение, полный доступ).
* Принтеры (печать, управление принтерами, управление документами, полный доступ).
* Общие сетевые ресурсы (чтение, изменение, полный доступ).
* Разделы реестра (запрос значения, задание значения, создание подраздела, удаление, смена владельца).
* Службы (пуск, останов, опрос состояния, смена разрешений, полный доступ).
* Объекты групповой политики GPO (разрешения определяют применение фильтра к групповой политике в соответствии с членством в группе безопасности, то есть применять данный GPO к членам определенной группы или нет).
* Объекты Инструментария управления Windows WMI (авторизация пользователей и назначение разрешений на выполнение методов, доступ на чтение и запись объектов и классов, удаленный доступ к пространству имен).
* Объекты DCOM (разрешения на запуск и активацию, локальный и удаленный доступ, разрешения на изменения настроек).
* Объекты IPC (мьютексы, семафоры, каналы и др. управляются на программном уровне системными вызовами).
* Кроме того, ядро Windows также создает большое число объектов разного типа, включая объекты-процессы, объекты-драйверы, объекты диспетчеризации и др. Проявляют себя на уровне системного программирования.

Типы субъектов:

* Локальные субъекты безопасности (группы и учетные записи) создаются на локальном компьютере, и использовать их можно для управления доступом к ресурсам, находящимся только на этом компьютере. Данные субъекты доступны только на компьютере-члене домена. Предопределённые субъекты имеют короткий well-known SID, добавленные имеют длинный SID,связанный с конкретным компьютером.
* Встроенные субъекты безопасности из контейнера Builtin заменяют локальные субъекты рядового сервера и могут быть использованы для управления доступа только на данном контроллере домена. Предоставление доступа к сетевому ресурсу данным субъектам недоступно из-за их области действия.
* Доменные субъекты безопасности могут быть использованы для ограничения/разрешения доступа к ресурсам по сети, поскольку они имеют уникальные SID’ы.