МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУГРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ им. проф. М.А. БОНЧ-БРУЕВИЧА»

Факультет Информационных систем и технологий
Кафедра Информационных управляющих систем

ОТЧЕТ

ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

проф., д.т.н.		Н.Н. Мошак
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ЛАБОРАТОРНАЯ РАБОТА № 2

«ГРУППОВЫЕЫЕ ПОЛИТИКИ БЕЗОПАСНОСТИ АРМ»

по курсу: Безопасность информационных технологий и систем

РАБОТУ ВЫПОЛНИЛ(А)

СТУДЕНТ(КА) ГР. _____ _____ _____

подпись, дата инициалы, фамилия

Санкт-Петербург

2023

Цель – изучить редактор локальной групповой политики и научиться настраивать групповые политики безопасности на автономном автоматизированном рабочем месте (АРМ) пользователя с установленной на нем операционной системой Windows для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: операционная система Windows XP.

2. Основные сведения

Введение в групповые политики Windows. Как системным администраторам в предприятиях, так и домашним пользователям рано или поздно приходится настраивать компьютеры, а также конфигурацию пользовательских учетных записей. В домашних условиях вы можете просто применить к своему компьютеру и необходимым учетным записям твики реестра, при помощи которых большинство настроек будут применены после перезагрузки компьютера или настраивать его вручную, что может занять очень много времени. Но как же быть, если вы работаете администратором в крупной компании, где нужно настроить десятки, а может и сотни компьютеров? Причем, в вашей организации, скорее всего, существует несколько отделов, у каждого из которых должны быть индивидуальные настройки. Например, компьютеры, расположенные в конференц-залах, предназначенные для проведения презентаций должны быть оснащены обоями рабочего стола с корпоративным логотипом. Или сотрудники отдела маркетинга не должны иметь права на запуск оснастки служб системы или редактора системного реестра. Большинство настроек локального компьютера, а также компьютеров, которые входят в состав доменной сети, настраиваются при помощи групповых политик.

Групповые политики - это набор правил, обеспечивающих инфраструктуру, в которой администраторы локальных компьютеров и доменных служб Active Directory могут централизовано развертывать и управлять настройками пользователей и компьютеров в организации. Все настройки учетных записей, операционной системы, аудита, системного реестра, параметров безопасности, установки программного обеспечения и прочие параметры развертываются и обновляются в рамках домена при помощи параметров объектов групповой политики GPO (Group Policy Object). Групповые политики являются компонентом операционной системы Windows и основываются на тысячах отдельных параметров политик, иначе говоря, политик, определяющих определённую конфигурацию для своего применения.

История групповых политик

Для операционных систем Windows концепция групповых политик не является инновационным шагом в области системной безопасности и настройки операционных

систем. Первые политики появились еще в Windows NT 4.0 и назывались системными политиками. Эти политики предназначались только для изменения данных системного реестра и основывались на файлах, которые назывались шаблонами adm. Для создания этих политик использовался специальный редактор системных политик. На то время системные политики были значительным шагом в обеспечении безопасности операционных систем Windows, несмотря на то, что объекты локальной политики не использовались, и система Windows NT 4.0 не поддерживала службы Active Directory.

Групповые политики появились в операционной системе Windows 2000 и включали в себя около 900 настроек для пользователей и компьютеров, которые могли в полной мере применяться к клиентским компьютерам. Из утилиты, предназначенной для изменения данных системного реестра, групповые политики операционной системы Windows 2000 превратились в компонент, предназначенный для изменения параметров конфигурации операционной системы. Групповые политики по-прежнему расположены в шаблонах ADM. Система Windows 2000 Server уже позволяет распространять объекты групповых политик для компьютеров, расположенных в домене и подразделениях (OU) в Active Directory.

В операционных системах Windows XP и Windows Server 2003 возможности групповых политик были расширены. С появлением этих систем у администраторов появилась возможность управлять параметрами безопасности и установкой приложений, а количество политик увеличилось до 1400. Локальные объекты групповой политики существовали независимо от того, входит ли компьютер в состав домена, рабочей группы или вовсе не принадлежит к сетевой среде. Все это объекты хранились в папке %SystemRoot%\System32\Group Policy. Политики распространялись только на тот компьютер, где хранятся сами GPO. В том случае, если компьютер не принадлежал к домену, локальная политика использовалась только для настройки конфигурации локального компьютера. Но если он входил в состав домена Active Directory, то параметры, привязанные к инфраструктурной единице домена (домен, лес, сайт) заменяли параметры локального объекта групповой политики.

Операционные системы Windows Vista и Windows Server 2008 уже поддерживают около 2500 настроек групповых политик. Новые категории управления политиками теперь уже обеспечивают управление питанием, возможность блокировки установки устройств, улучшенные параметры безопасности, расширение настроек Internet Explorer, а также возможность делегировать пользователям право устанавливать драйверы принтеров. В этих операционных системах было создано расширение для формата шаблонов политик. У

форматов adm был значительный недостаток - для реализации локализации групповых политик нужно было создавать отдельный adm-файл для каждого языка. Теперь административные шаблоны представляют собой пару XML-файлов - *.admx файл, который определяет изменения в реестре, а также .adml файл, который отвечает за языковые настройки указанной политики. Несмотря на эти изменения, в одной системе могут сосуществовать как adm, так и admx/adml шаблоны без всяких проблем. В операционной системе Windows Server 2008 можно создавать стартовые объекты групповой политики. Использование стартового объекта групповой политики позволяет хранить набор параметров административных шаблонов политик в одном объекте и включать эти параметры в новые объекты групповой политики. Также для каждого объекта групповых политик появились возможности добавления комментариев, а сведения о подключенных сетях обеспечивают улучшение отклика групповой политики на изменение сетевых условий.

В операционных системах Windows 7 и Windows Server 2008 R2 уже насчитывается около 3200 настроек групповых политик.

2.1. Оснастка "Редактор локальной групповой политики".

Объекты групповых политик делятся на две категории:

"Доменные объекты групповых политик», которые используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена Active Directory. Эти объекты хранятся только на контроллере домена;

"Локальные объекты групповых политик», которые позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере. Эти объекты хранятся только в локальной системе. Локальные объекты групповых политик могут применяться, даже если компьютер входит в состав домена.

Для управления локальными объектами групповых политик в операционных системах Windows используется оснастка консоли управления **"Редактор локальной групповой политики"**. При помощи данной оснастки вы можете настраивать большинство системных компонентов и приложений. Рассмотрим подробно методы управления компьютером и пользователями при помощи данной оснастки. Вы можете открыть данную оснастку несколькими способами:

1.Нажмите на кнопку "**Пуск"** для открытия меню, в поле поиска введите Редактор локальной групповой политики и откройте приложение в найденных результатах;

2.Воспользуйтесь комбинацией клавиш +R для открытия диалога "**Выполнить"**. В диалоговом окне "**Выполнить**", в поле "**Открыть"** введите ***gpedit.msc*** и нажмите на кнопку "**ОК**";

3.Откройте **"Консоль управления ММС".** Для этого нажмите на кнопку **"Пуск",** в поле поиска введите ***mmc***, а затем нажмите на кнопку **"Enter".** Откроется пустая консоль ММС. В меню "**Консоль**" выберите команду "Добавить или удалить оснастку" или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге **"Добавление и удаление оснасток"** выберите оснастку "**Редактор объектов групповой политики"** и нажмите на кнопку **"Добавить"**. В появившемся диалоге **"Выбор объекта групповой политики"** нажмите на кнопку "**Обзор"** для выбора компьютера или нажмите на кнопку **"Готово"** (по умолчанию установлен объект **"Локальный компьютер"**). В диалоге "Добавление или удаление оснасток" нажмите на кнопку "ОК";

В оснастке редактора локальных объектов групповой политики присутствуют два основных узла:

2.1. Узел "**Конфигурация компьютера**», который предназначен для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, невзирая на то, под какой учетной записью пользователь вошел в систему. Эти параметры применяются при запуске операционной системы и обновляются в фоновом режиме каждые 90-120 минут.

Узел "**Конфигурация компьютера**» содержит ***три дочерних узла***, при помощи которых настраиваются все параметры локальных объектов групповых политик: ***Конфигурация программ, Конфигурация Windows, Административные шаблоны.***

2.2. **"Конфигурация пользователя»**, который предназначен для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему. Так же, как и параметры, расположенные в узле конфигурации компьютера, параметры, расположенные в узле конфигурации пользователя обновляются в фоновом режиме каждые 90-120 минут.

Узел "**Конфигурация пользователя**» также содержит ***три дочерних узла***, при помощи которых настраиваются все параметры локальных объектов групповых политик: ***Конфигурация программ, Конфигурация Windows, Административные шаблоны.***

В дочернем узле «***Конфигурация программ»*** расположено только одно расширение клиентской стороны *"Установка программ",* благодаря которому, вы можете указать определенную процедуру установки программного обеспечения. Расширения клиентской

стороны (Client-Side-Extension CSE) преобразовывает указанные параметры в объект групповой политики и вносит изменения в конфигурацию пользователя или компьютера. Создавать объекты групповой политики для развертывания программного обеспечения можно только в операционной системе Windows Server 2008/2008R2.

Дочерний узел ***"Конфигурация Windows"*** в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики. В нем вы можете найти несколько опций безопасности «Политика разрешения имен», «Сценарии», «Развернутые принтеры», «Параметры безопасности». Особый интерес представляет опция "Параметры безопасности". Эта опция позволяет настраивать политики безопасности средствами GPO. В этой опции для конфигурации безопасности компьютера доступны следующие настройки политик:

- *Политики учетных записей*, которые позволяют устанавливать политику паролей и блокировки учетных записей.
- *Локальные политики (можно не настраивать см ЛАБ№1)*, отвечающие за политику аудита, параметры безопасности и назначения прав пользователя.
- *Политики открытого ключа*, которые позволяют:

"настраивать компьютеры на автоматическую отправку запросов в центр сертификации предприятия и установку выдаваемых сертификатов;

"создавать и распространять список доверия сертификатов (CTL);

"добавлять агенты восстановления шифрованных данных и изменение параметров политики восстановления шифрованных данных;

"добавлять агенты восстановления данных шифрования диска BitLocker.

- *Политики ограниченного использования программ*, позволяющие осуществлять идентификацию программ и управлять возможностью их выполнения на локальном компьютере, в подразделении, домене и узле.
- *Политики управления приложениями*, отвечающие за создание и управления правилами и свойствами функционала AppLocker, который позволяет управлять установкой приложений и сценариев.
- *Политики IP-безопасности на "Локальный компьютер",* которые позволяют создавать политику IP-безопасности локального компьютера и управлять списками IP-фильтров.

Дочерний узел ***"Административные шаблоны"*** является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows. Каждому параметру политики административных шаблонов соответствует определенный параметр системного

реестра. Политики в дочернем узле ***"Административные шаблоны"*** узла **«Конфигурация компьютера»** изменяют значения реестра в ключе HKEY_LOCAL_MACHINE (или просто HKLM), а политики в дочернем узле ***"Административные шаблоны"*** узла **«Конфигурация пользователя»** - HKEY_CURRENT_USER (HKCU). В некоторых источниках административные шаблоны могут называться политиками на основе реестра. В рамках этой работы будет рассматриваться дочерний узел ***"Административные шаблоны"*** для локального компьютера. О применении настроек административных шаблонов для нескольких компьютеров или пользователей, входящих в домен, в данной работе не обсуждается.

Для системных администраторов дочерний узел ***"Административные шаблоны"*** предоставляет возможности динамического управления операционной системой. Несмотря на то, что администратору понадобится немало времени на настройку этого узла, все изменения, примененные при помощи групповых политик, невозможно будет изменить средствами пользовательского интерфейса.

3. Содержание работы

3.1. Провести настройки опций и политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя». При настройке опции «Сценарий» использовать сценарии на языках программирования и сценарии PowerShell (в пункте контекстного меню для свойства «Автозагрузка» выбрать вкладку - «Сценарии PowerShell».

3.2. Сформулировать выводы о значимости настроенной каждой политики для защиты АРМ от НСД

4. Содержание отчета

4.1.Цель работы

4.2. Основные сведения

4.3. Указать последовательность команд для выхода в диалоговые окна настройки параметров для каждой политики безопасности дочерних узлов. Пример: Откроем «Редактор локальной групповой политики», перейдя по адресу: «Конфигурация компьютера»→«Конфигурация Windows»→«Параметры безопасности» → «Политики учетных записей» →«Политики паролей»

4.4. Привести скриншоты до и после настройки параметров соответствующих политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя». Для опции

«Сценарий» привести скриншоты сценариев на языках программирования и сценариев PowerShell (в пункте контекстного меню для свойства «Автозагрузка» выбрать вкладку - «Сценарии PowerShell».

4.5. Обосновать настройки каждого параметра политик безопасности и сформулировать выводы о значимости настроенной политики для защиты АРМ от НСД

4.6. Сформулировать общий вывод значимости настроек групповой политики безопасности для защиты АРМ от НСД.