

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Филиал федерального государственного бюджетного образовательного
учреждения высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.» в г. Петровске



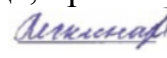
МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

по дисциплине

МДК 04.02. «Обеспечение качества функционирования
компьютерных систем»

направление подготовки

09.02.07 «Информационные системы и программирование»

Методические указания рассмотрены
на заседании предметной (цикловой)
комиссии общепрофессиональных
дисциплин, профессиональных модулей
специальностей технического профиля
«14» июня 2023 года, протокол №12
Председатель ПЦК /Лескина Т.А./

Петровск 2023

Пояснительная записка

Методические указания по выполнению лабораторных работ подготовлены на основе рабочей программы учебной дисциплины МДК.04.02 «Обеспечение качества функционирования компьютерных систем», разработанной на основе ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование» и соответствующих общих (ОК) и профессиональных (ПК) компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 10. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

ПК 4.1. Осуществлять установку, настройку и обслуживание программного обеспечения компьютерных систем

ПК 4.2. Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

При выполнении лабораторных работ студент должен *знать*:

– основные методы и средства эффективного анализа функционирования программного обеспечения;

- основные виды работ на этапе сопровождения программного обеспечения;
 - основные принципы контроля конфигурации и поддержки целостности конфигурации программного обеспечения;
 - средства защиты программного обеспечения в компьютерных системах
- При выполнении лабораторных работ студент должен *уметь*:
- подбирать и настраивать конфигурацию программного обеспечения компьютерных систем;
 - использовать методы защиты программного обеспечения компьютерных систем;
 - проводить инсталляцию программного обеспечения компьютерных систем;
 - производить настройку отдельных компонентов программного обеспечения компьютерных систем;
 - анализировать риски и характеристики качества программного обеспечения

Содержание лабораторных работ определено рабочей программой и тематическим планированием, соответствует теоретическому материалу изучаемых разделов учебной дисциплины.

Объем лабораторных работ по дисциплине определяется учебным планом по данной специальности.

Продолжительность лабораторной работы – 2 академических часа. Перед проведением лабораторной работы преподавателем организуется инструктаж, а по ее окончании – обсуждение итогов.

Комплект методических указаний по выполнению лабораторных работ по дисциплине МДК.04.02 «Обеспечение качества функционирования компьютерных систем» содержит 3 лабораторных занятий.

**Перечень лабораторных работ
по дисциплине МДК.04.02 «Обеспечение качества функционирования
компьютерных систем»**

ЛАБОРАТОРНАЯ РАБОТА № 1.

Тема: Установка и настройка антивируса. Настройка обновлений с помощью зеркала

ЛАБОРАТОРНАЯ РАБОТА № 2.

Тема: Настройка политики безопасности

ЛАБОРАТОРНАЯ РАБОТА № 3.

Тема: Настройка браузера

ЛАБОРАТОРНАЯ РАБОТА № 1

Тема: Установка и настройка антивируса. Настройка обновлений с помощью зеркала

Цель работы: научиться устанавливать и настраивать антивирусную программу на ПК, настраивать обновления с помощью зеркала.

Оборудование: ПК, интернет, программное обеспечение – антивирусная программа, инструкции по выполнению работы

Порядок выполнения работы:

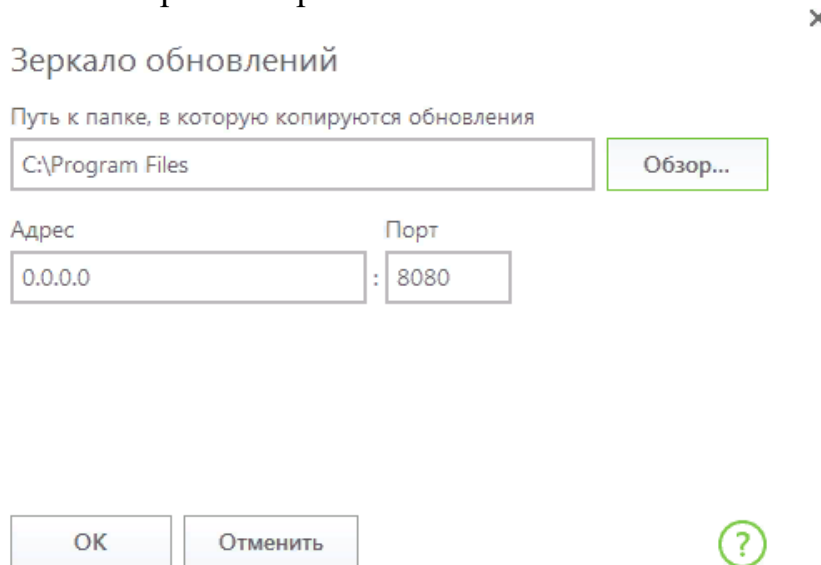
Задание 1. Установить и настроить антивирусную программу на выбор Avast, DrWed, Nod32

Задание 2. Настроить обновления антивирусной программы с помощью зеркала.

Зеркало обновлений – это компьютер, настроенный как источник обновлений для антивируса на других ПК в локальной сети. Используется в сетях, где не все ПК имеют доступ в Интернет.

Для создания зеркала обновлений:

1. Откройте меню антивируса, щёлкнув по значку в трее и выбрав *Центр безопасности*;
2. Щёлкните по значку замка, разрешите внесение изменений и нажмите кнопку с шестерёнкой (*Настройки*)
3. Перейдите на вкладку *Обновление* и выберите *Дополнительные настройки*.
4. Установите переключатель *Зеркало обновлений* в положение *Вкл*.
Открывается окно настройки зеркала:



5. Нажмите *Обзор* и укажите папку, куда будут сохраняться обновления. Она будет источником обновления для остальных ПК в локальной сети.
6. *Адрес* – адрес данного ПК в локальной сети, который будет использоваться как адрес для обновления через антивирусную сеть другими ПК в этой сети. *Порт* – номер порта, который будет использоваться для раздачи обновлений.

ЛАБОРАТОРНАЯ РАБОТА № 2

Тема: Настройка политики безопасности

Цель работы: изучение основных средств администрирования учетных записей пользователей в семействе ОС Windows и групп пользователей. Настройка локальной политики безопасности: пользователей, паролей, блокировки учетной записей, прав пользователей и настроек безопасности операционной системы.

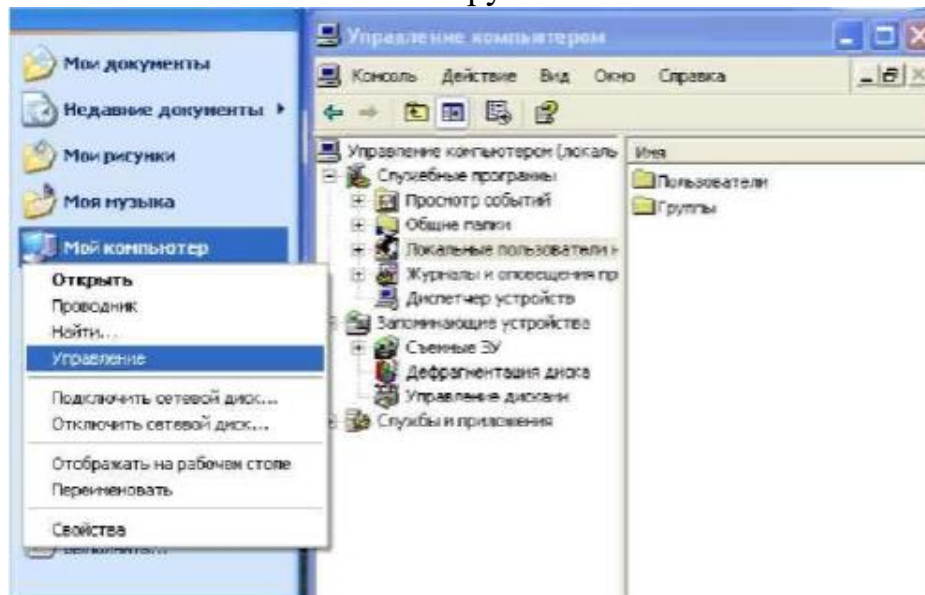
Оборудование: ПК, интернет, программное обеспечение – операционная система Windows 7, MS Word, инструкции по выполнению работы

Порядок выполнения работы:

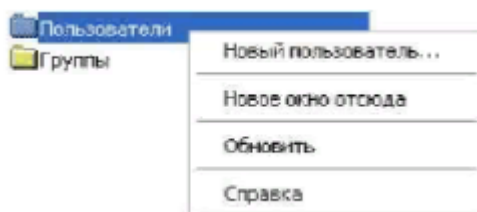
Задание. Создать и настроить учетную запись пользователя. Настроить локальную политику безопасности для пользователя.

1. Управление учётными записями локальных пользователей

1.1 В контекстном меню значка «Мой компьютер» откройте «Управление». Выберите «Локальные пользователи и группы»



1.2. В контекстном меню папки «Пользователи» правой половины окна (или в меню «Действие») выберите элемент «Новый пользователь»,



Создайте учётную запись пользователя. Если требуется смена пароля при следующем входе в систему, установите флажок «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь получает запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей. Если установлен этот флажок, вы не можете установить флажки «Запретить смену пароля пользователем» и «Срок действия пароля не ограничен».

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить старый пароль при помощи функции «Задать пароль».

Имя| Полное имя

Help Assistant Учетная запись помощи,,.

5UPPORT_38... CN=Microsoft Corporation...

Ддминистра...

Удалить

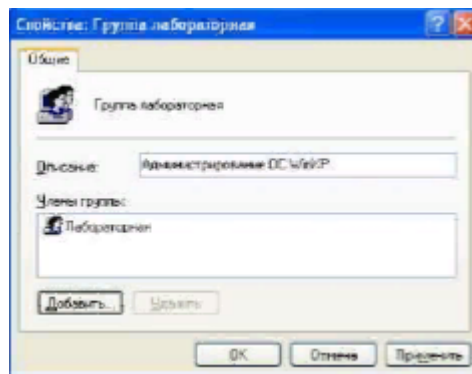
Переименовать

Свойства

Справка

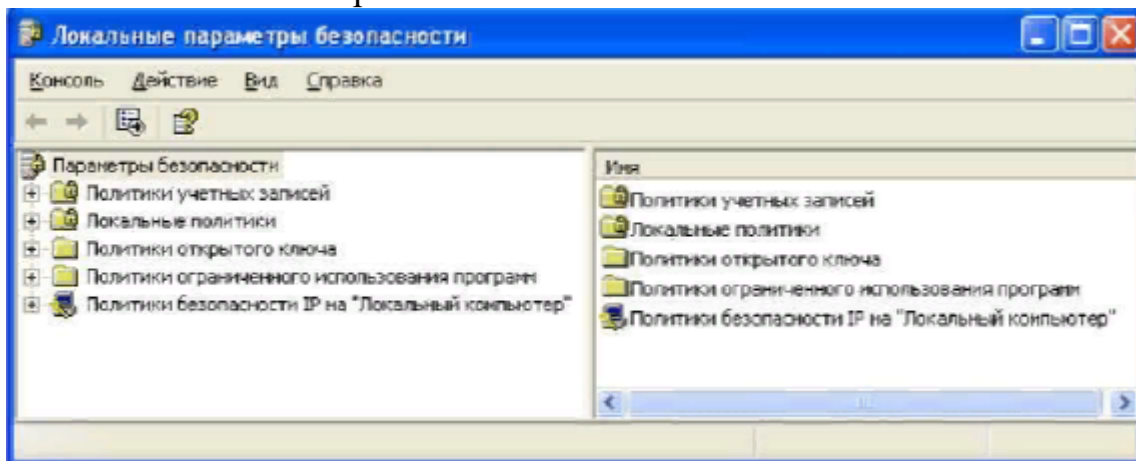
1.3. Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи».

1.4. В папке «Группы» откройте свойства группы «Опытные пользователи» и проверьте наличие в группе только что добавленного пользователя. Создайте новую группу и добавьте в неё этого же пользователя.

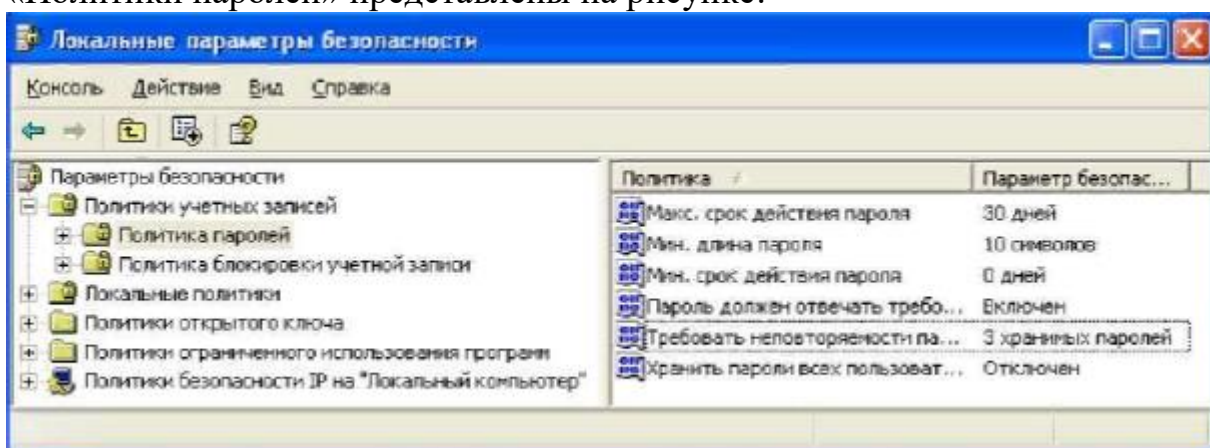


2. Настройка локальной политики безопасности

2.1. Откройте оснастку «Локальная политика безопасности». (Пуск - Панель управления - Администрирование - Локальная политика безопасности). Главный вид окна оснастки представлен на рисунке. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.



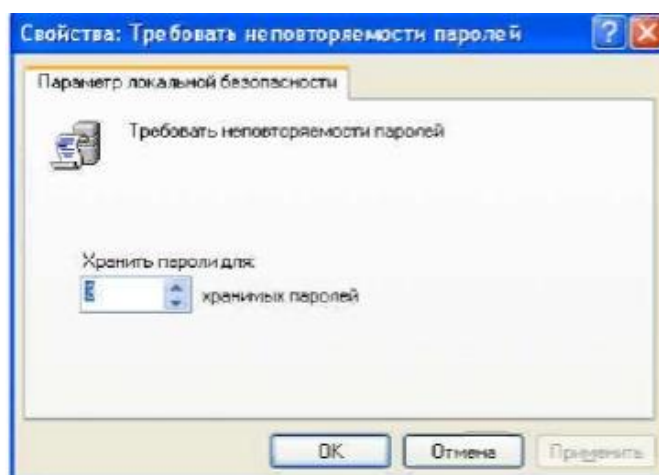
2.2. Выберите раздел «Политики паролей». (Параметры безопасности - Политики учётных записей - Политики паролей). Настройки, входящие в раздел «Политики паролей» представлены на рисунке:



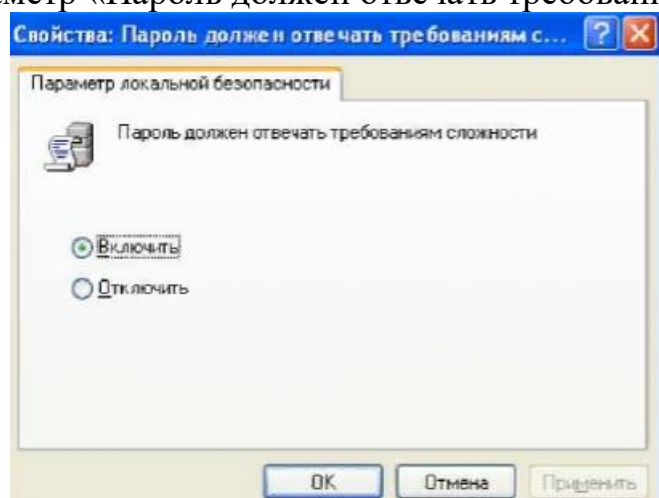
2.3. Установите максимальный срок действия пароля - 30 дней.

Установите минимальную длину пароля - 10 символов.

Для параметра «Требовать неповторяемости паролей» установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя.



2.4. Включите параметр «Пароль должен отвечать требованиям сложности»

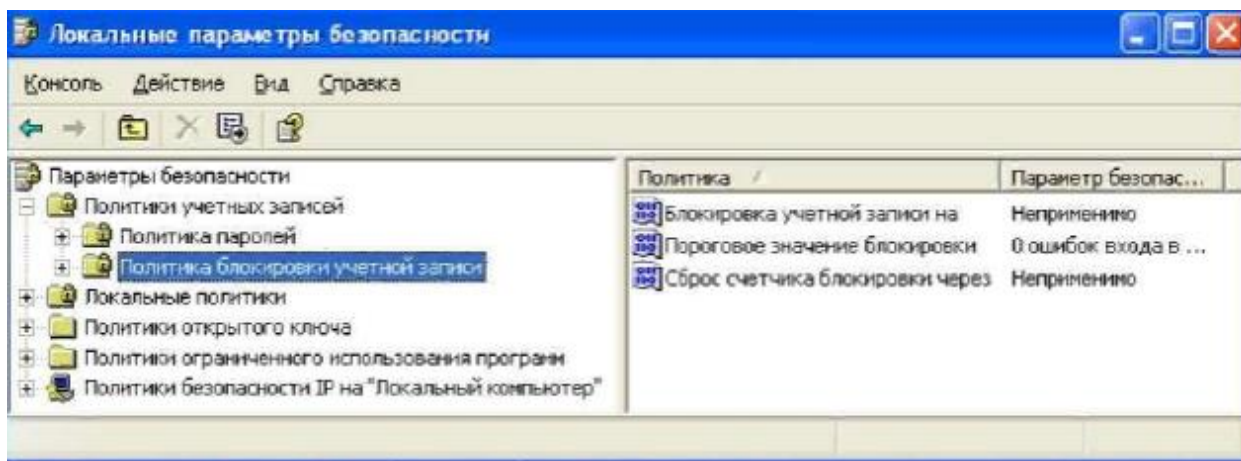


Примечание: этот параметр безопасности определяет требования сложности для паролей. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из шести символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:
 - прописные буквы английского алфавита от А до Z;
 - строчные буквы английского алфавита от а до z;
 - десятичные цифры (от 0 до 9);
 - неалфавитные символы (например, !, \$, #, %).

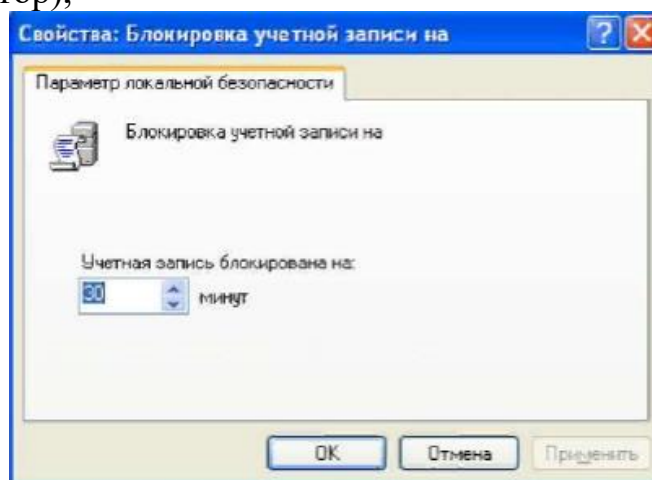
Проверка соблюдения этих требований выполняется при изменении или создании паролей. Таким образом, можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т.д.

2.5. Выберите раздел «Политика блокировки учётной записи» (Параметры безопасности - Политики учётных записей – Политика блокировки учетной записи). У созданной учетной записи попытайтесь заменить пароль на более простой (например: abc12345) после чего на пароль удовлетворяющий требованиям.



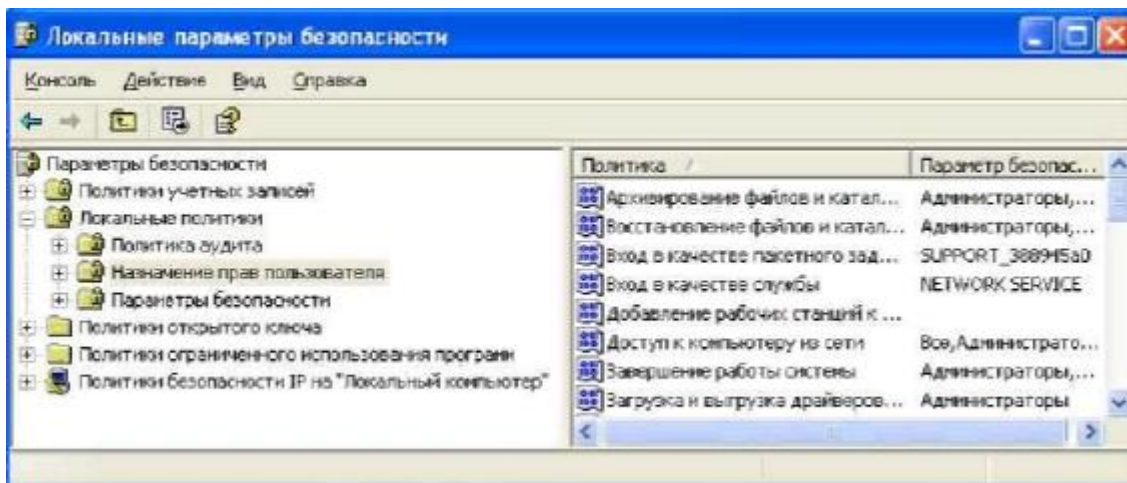
2.6. Настройте параметры следующим образом:

- установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется);
- установить длительность блокировки в параметре «Блокировка учётной записи на» равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

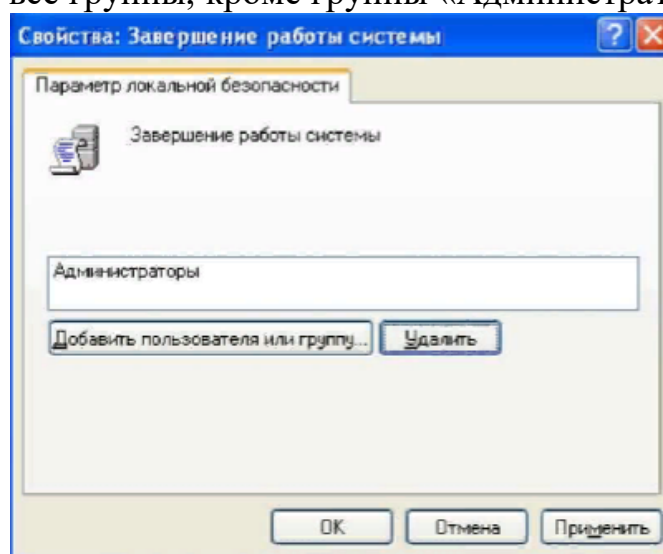


- установите сброс счётчика блокировки через 15 мин. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течении установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).

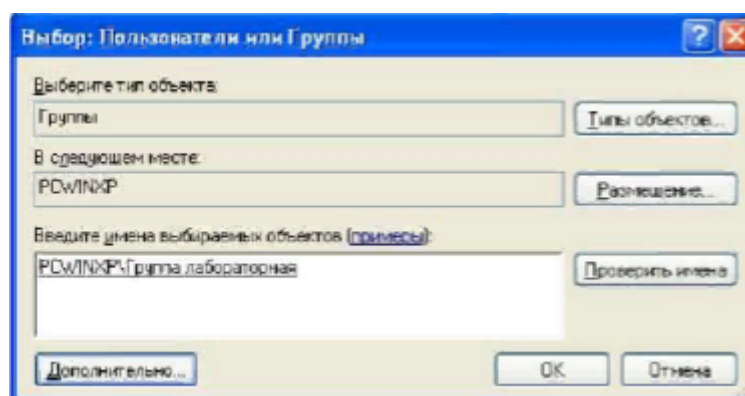
2.7. Выберите раздел «Назначение прав пользователя». (Параметры безопасности – Локальные политики - Назначение прав пользователя). При входе с систему под учетной записью пользователя 3 раза введите неправильный пароль. Разблокируйте учетную запись. Настройками этого раздела являются права, которыми можно наделять пользователей или группы пользователей (примеры прав: архивирование и восстановление файлов и каталогов, загрузка и выгрузка драйверов устройств, изменение системного времени).



2.8.Присвоение права. «Завершение работы системы»: в свойствах выбранного параметра удалите все группы, кроме группы «Администраторы»;



Нажмите «Добавить пользователя или группу», затем кнопку «Типы объектов» и добавьте в параметры поиска тип «Группы»; выберите искомую группу.



Таким образом, пользователи, входящие в выбранную группу, в дополнение к правам групп «Пользователи» и «Опытные пользователи» получают право на завершение работы системы.

2.9.Проверьте возможность завершения работы системы пользователем созданным в п.1.2.

2.10.Под учетной записью администратора удалите созданного пользователя из группы, созданной в п. 1.4. Проверьте возможность завершения работы системы созданным пользователем.

2.11.Право «загрузка и выгрузка драйверов».

Этот параметр безопасности определяет, какие пользователи могут динамически загружать и выгружать драйверы устройств или другой код в режим ядра. Это право пользователя не применяется для драйверов устройств «Plug and Play».

2.12.Право «Закрепление страниц в памяти».

Этот параметр безопасности определяет, какие учетные записи могут использовать процесс для хранения данных в физической памяти, избегая подкачки страниц в виртуальную память на диске. Применение этой привилегии может существенно сказаться на системной производительности, поскольку приводит к уменьшению объема свободной оперативной памяти.

2.13.Право «Изменение системного времени».

Это право пользователя определяет, какие пользователи и группы могут изменять время и дату на встроенных часах компьютера. Пользователи, обладающие данным правом, могут изменять представление журналов безопасности. При изменении системного времени события будут заноситься в журнал с указанием измененного, а не реального времени.

2.14.Право «Локальный вход в систему».

Это право пользователя определяет пользователей, имеющих возможность интерактивно входить в систему. Данное право необходимо для входа пользователя в систему после одновременного нажатия клавиш CTRL+ALT+DEL на клавиатуре компьютера. Кроме того, это право на вход в систему может понадобиться некоторым службам или административным приложениям, во время работы которых происходит вход пользователей в систему.

2.15.Право «Отладка программ».

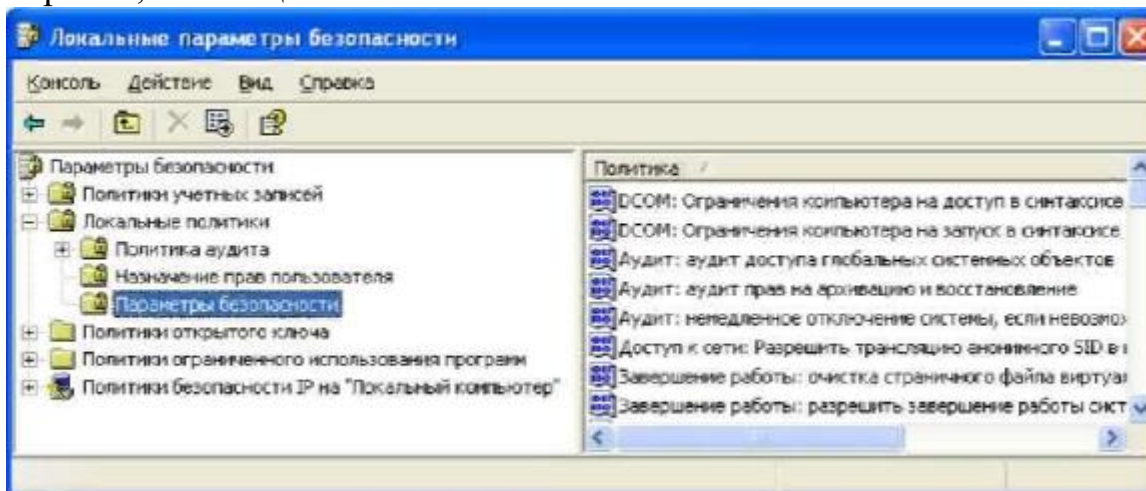
Это право пользователя определяет, какие пользователи могут запускать режим отладки для любого процесса или ядра. Разработчики, запускающие процесс отладки для собственных приложений, не нуждаются в предоставлении данного права пользователя. Данное право необходимо предоставить разработчикам, запускающим процесс отладки для новых системных компонент. Эта привилегия обеспечивает широкие возможности доступа к особо важным компонентам операционной системы.

2.16.Право «Увеличение приоритета диспетчирования».

Этот параметр безопасности определяет, какие учетные записи могут использовать процесс, обладающий разрешением «Запись свойства» для доступа к другому процессу, с целью повысить назначенный последнему приоритет выполнения. Пользователь, обладающий этой привилегией, может изменять приоритет планирования процесса в окне диспетчера задач.

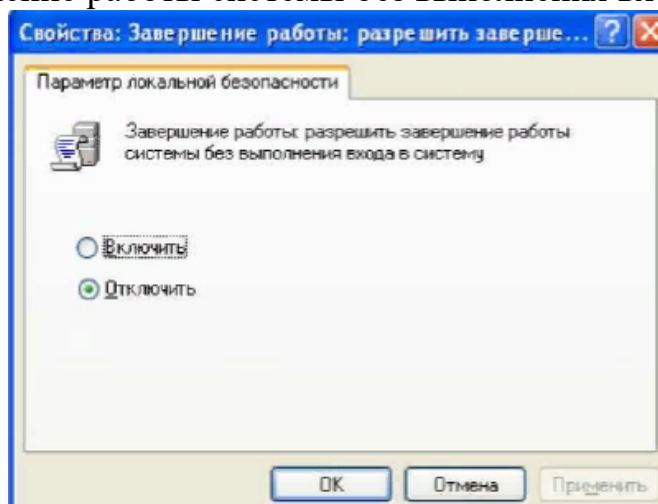
Выберите раздел «Параметры безопасности» (Параметры безопасности - Локальные политики - Параметры безопасности). Настройка параметров

раздела позволяет изменять настройки операционной системы, каким-либо образом, влияющие на безопасность.

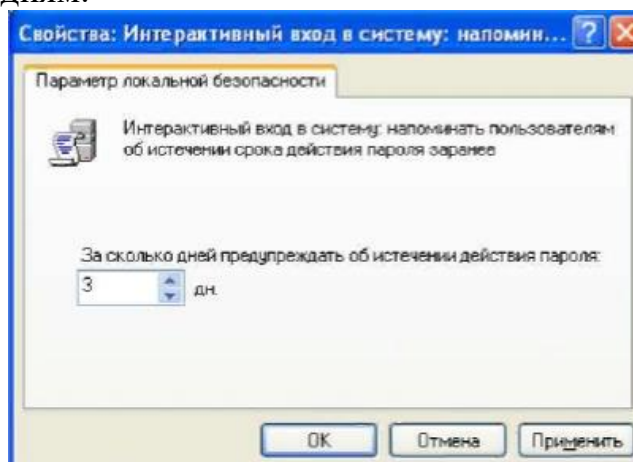


2.17.Измените следующие настройки.

Применительно к «Завершению работы», - отключить параметр «разрешить завершение работы системы без выполнения входа в систему»



Применительно к «Интерактивный вход в систему», - включите параметр «не отображать последнего имени пользователя» и установите значение параметра «напоминать пользователям об истечении срока действия пароля заранее», равным 3 дням.



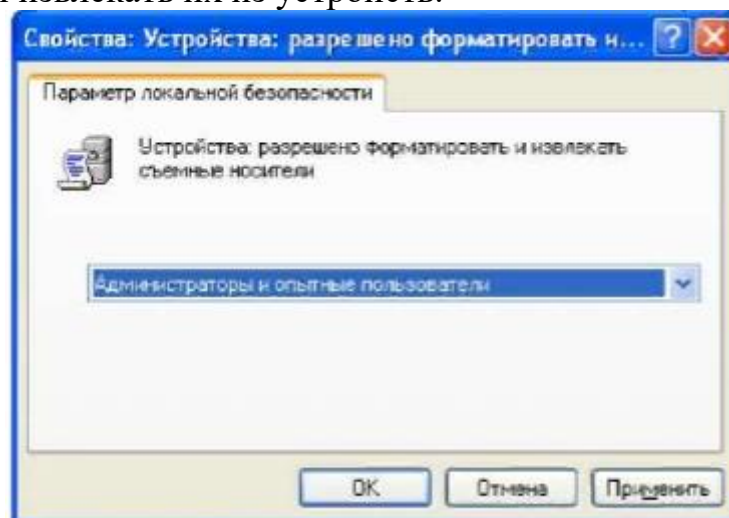
Применительно к «интерактивный вход в систему», отключите параметр «не требовать нажатия CTRL+ALT+DEL». Этот параметр безопасности

определяет, должен ли пользователь, прежде чем войти в систему, нажать клавиши CTRL+ALT+DEL. Если эта политика включена на компьютере, пользователь не должен для входа в систему нажимать CTRL+ALT+DEL. В таком случае компьютер становится уязвимым для атак, основанных на перехвате паролей пользователей. Если потребовать нажатия клавиш CTRL+ALT+DEL перед входом в систему, то пользователям будет гарантирован надежно защищенный канал передачи паролей.

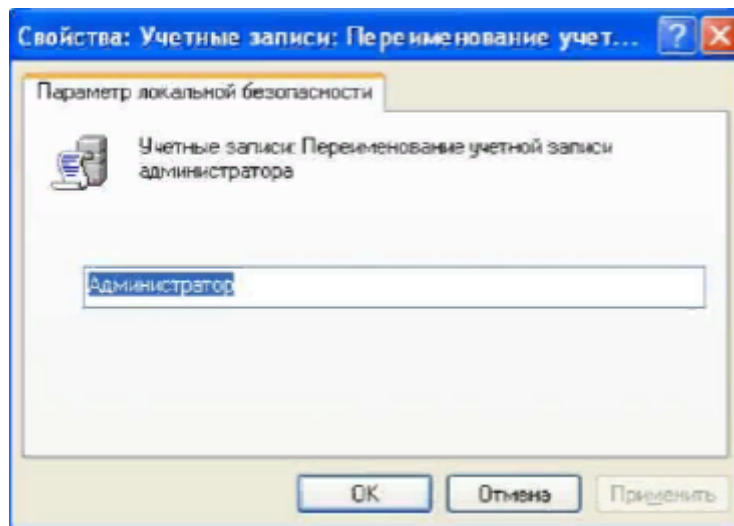
Если эта политика отключена, то любой пользователь должен будет перед входом в Windows нажимать CTRL+ALT+DEL (если только он не входит в систему с помощью смарт-карты).

Применительно к «Устройства», - включите параметр «запретить пользователю установку драйверов принтера». Чтобы локальный компьютер мог выполнять печать на сетевом принтере, необходимо установить на компьютере драйвер этого принтера. Данный параметр безопасности определяет, кому при добавлении сетевого принтера разрешается устанавливать драйвер принтера. Если параметр включен, то устанавливать драйвер при добавлении сетевого принтера разрешается только группам «Администраторы» и «Опытные пользователи». Если параметр отключен, то устанавливать драйвер при добавлении сетевого принтера может любой пользователь.

Применительно к «Устройства», - параметр «разрешено форматировать и извлекать съемные носители» разрешите группам пользователей «Администраторы», «Опытные пользователи». Этот параметр безопасности определяет каким пользователям разрешается форматировать съемные носители NTFS и извлекать их из устройств.



2.18. Измените параметр «Переименование учетной записи администратора», переименование учетной записи усложнит пользователям, не имеющим доступа в систему, процесс угадывания имени пароля пользователя с правами администратора. Этот параметр определяет, следует ли сопоставить идентификатору безопасности (SID) учетной записи Администратор другое имя учетной записи;



2.19. Проверьте наличие прав, которыми был наделён пользователь в п.2.4 (проверить возможность завершения работы системы; под учётной записью администратора удалить пользователя из группы, созданной в п. 1.4; проверить возможность завершения работы системы пользователем с учётной записью, созданной в п. 1.2). Также проверьте следующие настройки: завершение работы без входа в систему, срок действия пароля, не требовать нажатия CTRL+ALT+DEL, переименование учетной записи администратора и состояние учетной записи гость.

ЛАБОРАТОРНАЯ РАБОТА № 3

Тема: Настройка браузера

Цель работы: Изучить настройки браузера Internet Explorer. Научиться ускорять загрузку Web-страниц

Оборудование: ПК, интернет, программное обеспечение – браузер, MS Word, инструкции по выполнению работы

Справочный материал:

Программа, отображающая HTML-документ на конкретном компьютере называется браузером. Для эффективной работы в Интернете необходима настройка браузера. Начать настройку программы Internet Explorer можно из самой этой программы (*Сервис - Свойства обозревателя*), так и через общесистемное средство Windows – Панель управления (значок свойства обозревателя). Общие параметры браузера задаются на вкладке Общие. Здесь можно указать какую страницу следует использовать в качестве основной, задать объем дискового пространства для хранения временных файлов Интернета и удалить временные файлы, а также страницы, подготовленные для чтения в автономном режиме. Правила хранения временных файлов задаются с помощью кнопки Настройка. Управление оформлением отображаемых Web-страниц также осуществляется элементами управления вкладки Общие. Используемые цвета настраиваются при помощи кнопки Цвета, а шрифты – при помощи кнопки Шрифты. С помощью кнопки Оформление можно задать принудительное использование параметров форматирования, заданных в свойствах браузера. Настройка свойств соединения с Интернетом осуществляется при помощи вкладки Подключение. Средства защиты от потенциально опасного содержимого Web-документов предоставляет вкладка Безопасность. Она позволяет указать Web-узлы, взаимодействие с которыми следует считать опасным, и запретить прием с них информации, которая может оказаться разрушительной. Прочие настройки сосредоточены на вкладке Дополнительно. Они позволяют: соблюдать конфиденциальность работы с помощью средств шифрования, контролировать использование средств языка Java, управлять отображением мультимедийных объектов, использовать дополнительные настройки оформления, управлять режимом Web-страниц, содержащих нужную информацию.

Порядок выполнения работы:

1. Управление основными параметрами отображения Web-страниц.

- 1.1. Запустите программу Internet Explorer.
- 1.2. Дайте команду *Сервис - Свойства обозревателя*.
- 1.3. Выберите вкладку *Общие*. Введите следующую страницу, с которой надо начинать обзор: www.kbsu.ru.
- 1.4. Щелкните по кнопке *Настройка*, увеличьте размер папки с временными файлами Интернета до 70 Мб.
- 1.5. Щелкните по кнопке *Просмотр файлов*, просмотрите временные файлы, созданные на диске при загрузке страниц. Нажмите *Ок*.
- 1.6. Нажмите на кнопку *Удалить*, в появившемся окне поставьте флажок, напротив строки: удалить все содержимое. Нажмите *Ок*.

- 1.7. Установите 30 дней для хранения ссылок в журнале.
- 1.8. Щелкните по кнопке *Цвета*, измените цвет просмотренных и не просмотренных ссылок.
- 1.9. Нажмите кнопку *Шрифты* и в появившемся окне выберите набор знаков – *Кириллица*, установите любой шрифт для Web-страницы и обычного текста.
- 1.10. Нажмите кнопку *Языки*, добавьте *Русский язык, английский*.
- 1.11. Выберите вкладку *Безопасность*, изучите уровни безопасности, устанавливаемые для различных зон Интернета: Интернет, местная интрасеть, надежные узлы, ограниченные узлы.
- 1.12. Выберите вкладку *Содержание*, включите ограничение доступа к информации, получаемой из Интернета, установите 1 уровень для всех категорий страниц.
- 1.13. Перезапустите Internet Explorer. И просмотрите, как изменилась загрузка страниц. Сделайте вывод.

2. Настройка отображения объектов

- 2.1. Запустите программу Internet Explorer.
- 2.2. На панели Адрес введите: *http://physics.about.com*.
- 2.3. Щелкните на гиперссылке *Classical mechanics*.
- 2.4. Зафиксируйте с помощью секундомера время загрузки страницы.
- 2.5. Посмотрите, как выглядит загруженная страница.
- 2.6. Щелкните на кнопке *Назад* на панели инструментов.
- 2.7. Дайте команду *Сервис - Свойства обозревателя*.
- 2.8. Откройте вкладку *Дополнительно*.
- 2.9. Сбросьте флажки *Воспроизводить анимацию, Воспроизводить звуки, Воспроизводить видео и Отображать рисунки*.
- 2.10. Выберите вкладку *Общие*.
- 2.11. Щелкните на кнопке *Удалить файлы*.
- 2.12. Щелкните на кнопке *ОК*.
- 2.13. Опять щелкните на гиперссылке *Classical mechanics*.
- 2.14. Еще раз зафиксируйте с помощью секундомера время загрузки страницы.
- 2.15. Сравните результаты измерений.
- 2.16. Сравните внешний вид страницы при предыдущей и нынешней загрузке.
- 2.17. Щелкните на одной из пустых рамок для рисунков правой кнопкой мыши, и выберите в контекстном меню команду *Показать рисунок*.

Контрольные вопросы:

1. Что такое браузер, виды браузеров.
2. Ускорение загрузки Web - страниц.

Информационное обеспечение обучения по дисциплине

Основные учебные издания:

1. Извозчикова, В. В. Эксплуатация информационных систем: учебное пособие для СПО / В. В. Извозчикова. — Саратов: Профобразование, 2019. — 136 с. — ISBN 978-5-4488-0355-0. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/86210>
2. Методы и средства комплексной защиты информации в технических системах: учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 224 с. — ISBN 978-5-9515-0429-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/101925.html>

Электронно-библиотечная система:

3. ЭБС «IPRbooks», ООО «Ай Пи Ар Медиа»
4. ЭБС «Znanium»
5. ЭБС «PROФобразование»
6. ЭБС «Book.ru»