Министерство образования и науки Российской Федерации  
Государственное бюджетное образовательное учреждение высшего профессионального образования  
Российский государственный педагогический университет им. А. И. Герцена.

**Сети и телекоммуникации.**

**Лабораторная работа № 2.**

**УПРАВЛЕНИЕ ПОЛИТИКОЙ БЕЗОПАСНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS.**

Выполнил

студент 3 курса,   
института компьютерных наук   
и технологического образования

Бахурев Н.Ю.

Санкт-Петербург

2017 г.

Цель работы

Освоение средств администратора и аудитора операционной системы Windows.

Часть 1

**Аудит** - процесс, позволяющий фиксировать события, происходящие в операционной системе и имеющие отношение к безопасности.

**Журнал аудита** - запись в хронологическом порядке действий системы, содержащей достаточно сведений для того, чтобы реконструировать, проанализировать и проверить последовательность сред и действий, окружающих каждое событие или ведущих к каждому событию по ходу операции от ее начала до выдачи окончательных результатов.

**Цифровая подпись** - последовательность символов, полученная в результате криптографического преобразования электронных данных. ЭЦП добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки.

* **События**, которые должны быть занесены в журнал аудита:
  1. Вход в систему
  2. Управление учетной записью
  3. Доступ к службе каталогов
  4. Доступ к объектам
  5. Изменения политики
  6. Использования привилегий
  7. Отслеживание процессов
  8. Системных событий
* **Параметры**, определяющие политику аудита:
  1. Аудит вход в систему
  2. Аудит управление учетной записью
  3. Аудит доступ к службе каталогов
  4. Аудит доступ к объектам
  5. Аудит изменения политики
  6. Аудит использования привилегий
  7. Аудит отслеживание процессов
  8. Аудит системных событий
  9. Аудит событий входа в систему
* Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

*Безусловно, нет – это может привести к негативным результатам различной степени тяжести.*

* Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя?

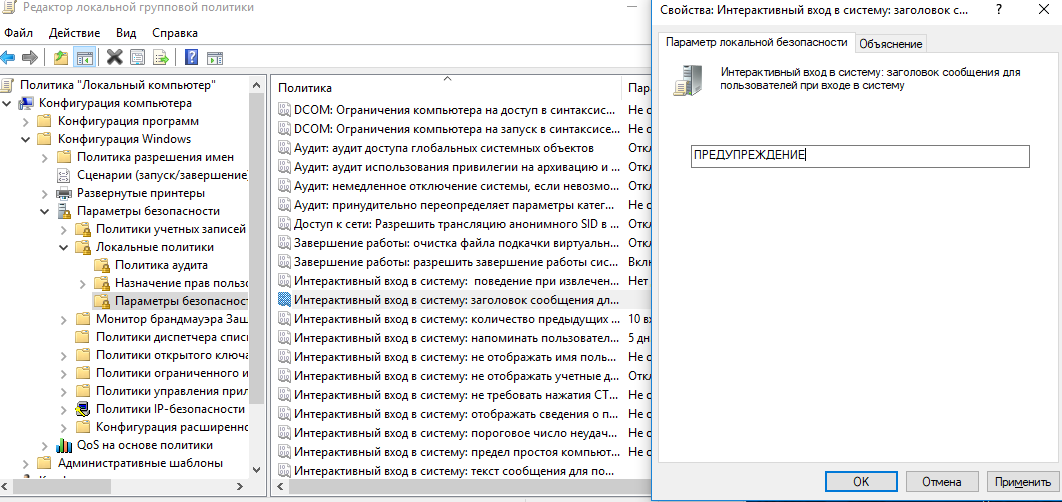
*В зашифрованном виде.*

* Нужно ли ограничивать права пользователей по запуску прикладных программ?

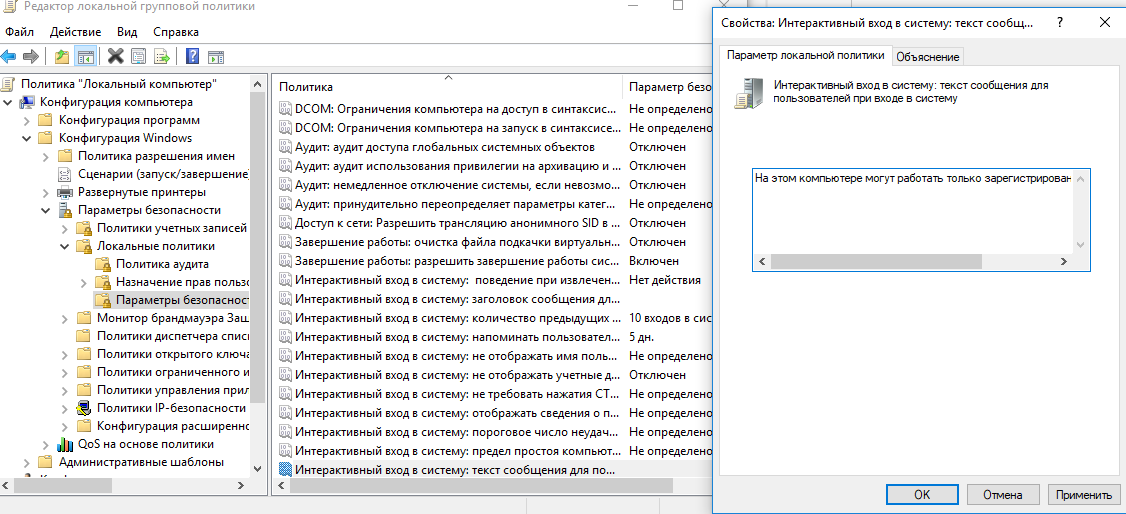
*Если этого не сделать, то велика вероятность заражения системы, особенно если речь идет о неопытном пользователе.*

Часть 2

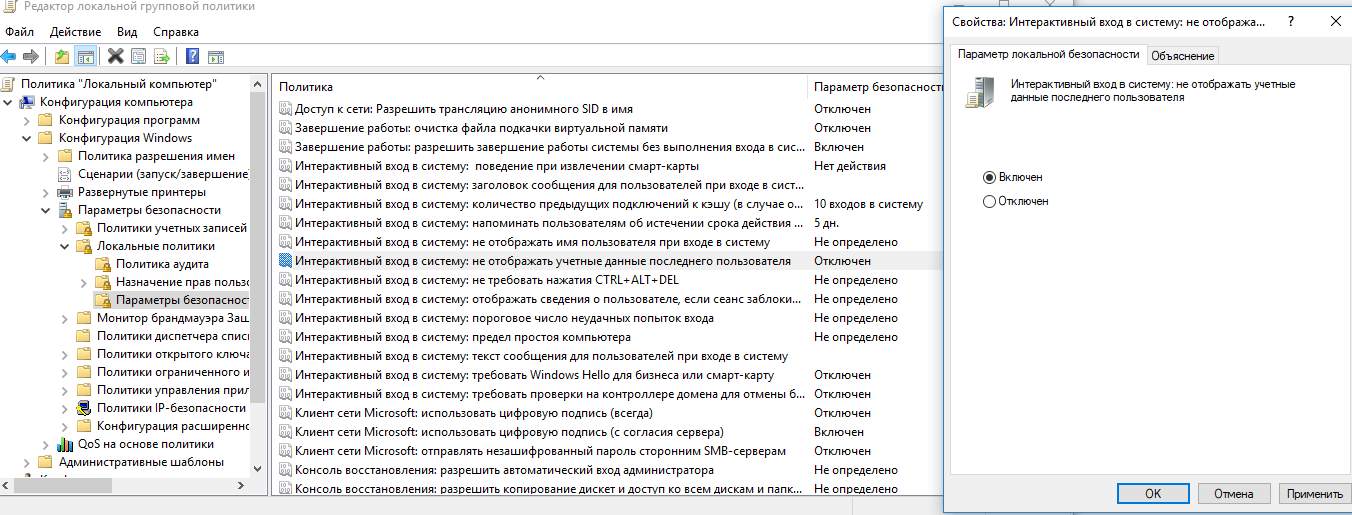
1. Установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»



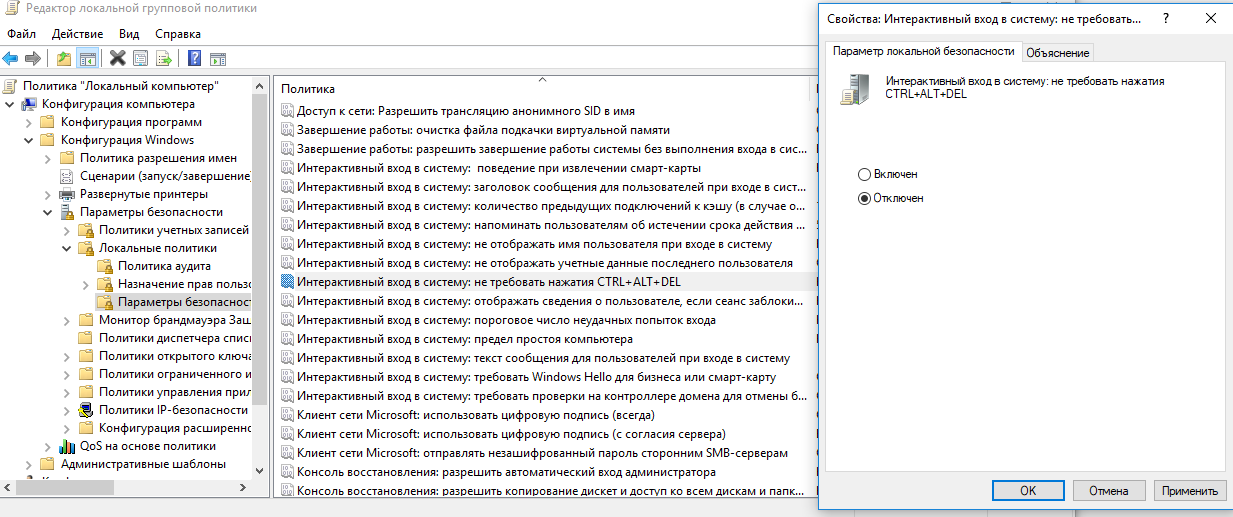
1. Установить текст «На этом компьютере могут работать только зарегистрированные пользователи!» в качестве значения параметра «Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»



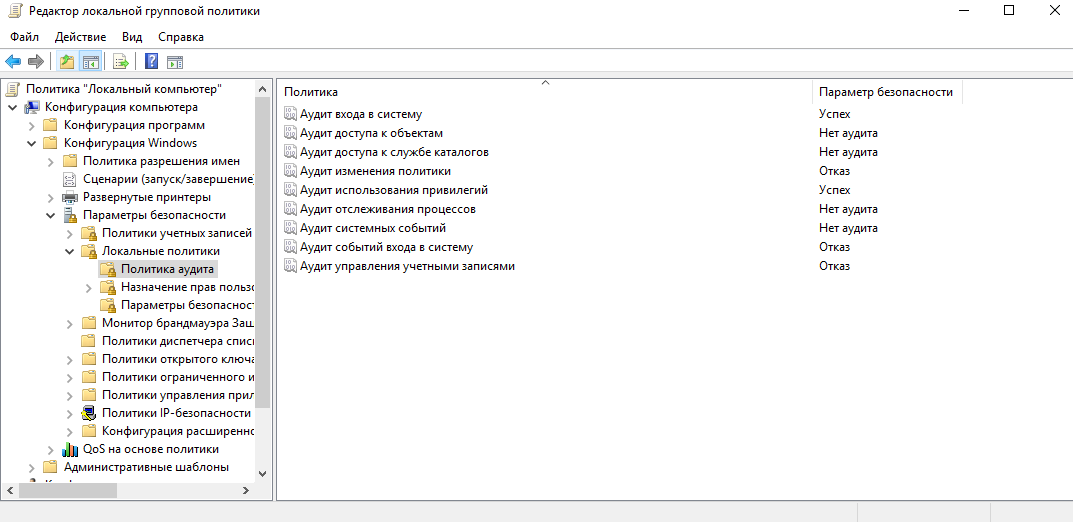
1. Установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя»



1. Установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»



1. У Параметры безопасности обеспечивают надежный вход в систему для пользователей данного ПК и ограничивают к нему доступ другим пользователям.
2. С помощью параметров политики аудита установить регистрацию в журнале аудита успешных и неудачных попыток:
   * входа в систему
   * изменения политики
   * использования привилегий
   * событий входа в систему
   * управления учетными записями



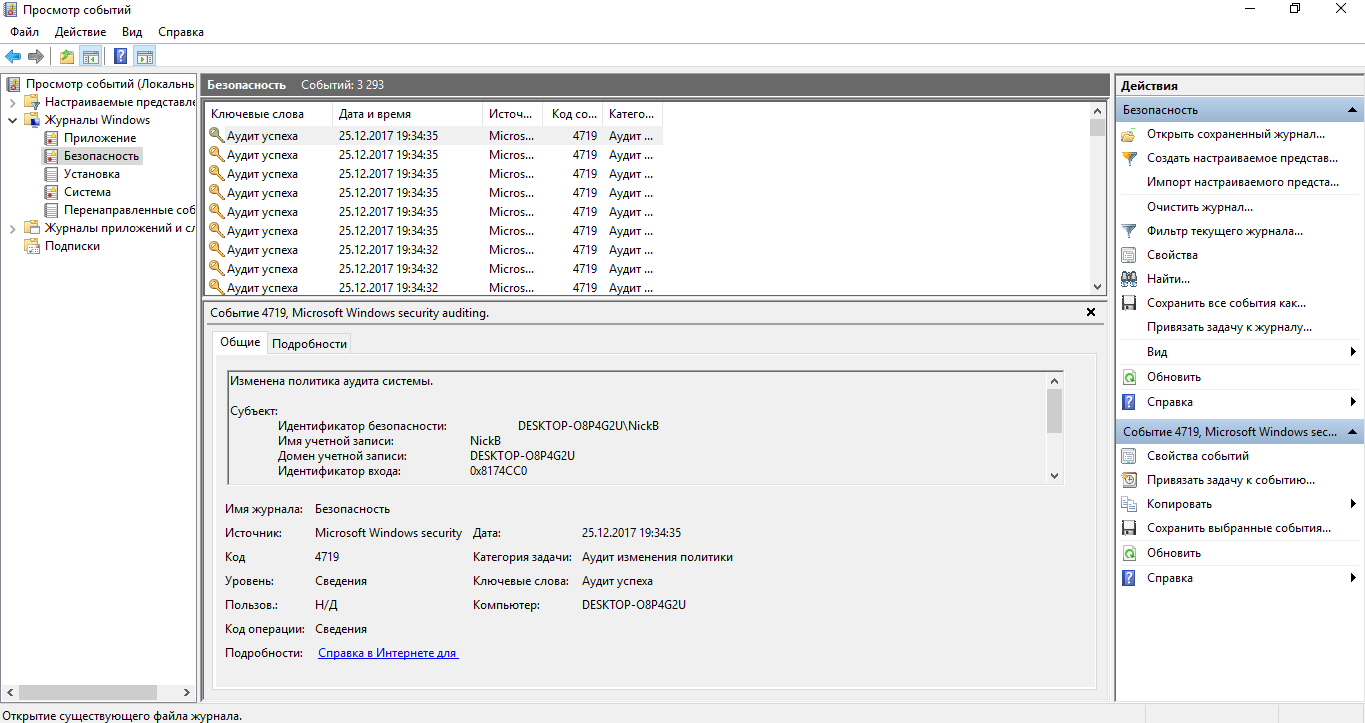
1. Журнал аудита событий безопасности расположен:

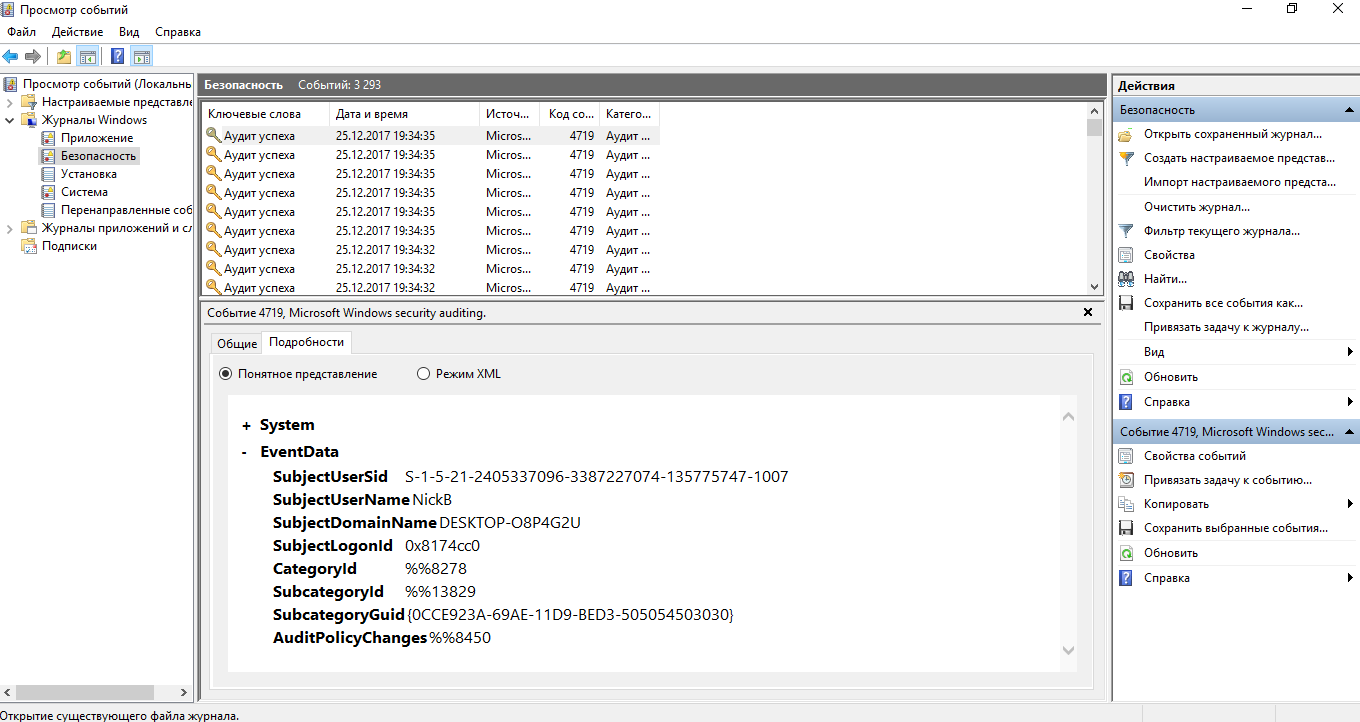
Панель управления> Администрирование> Просмотр событий> Безопасность

1. Какие ещё параметры политики аудита могут быть определены?

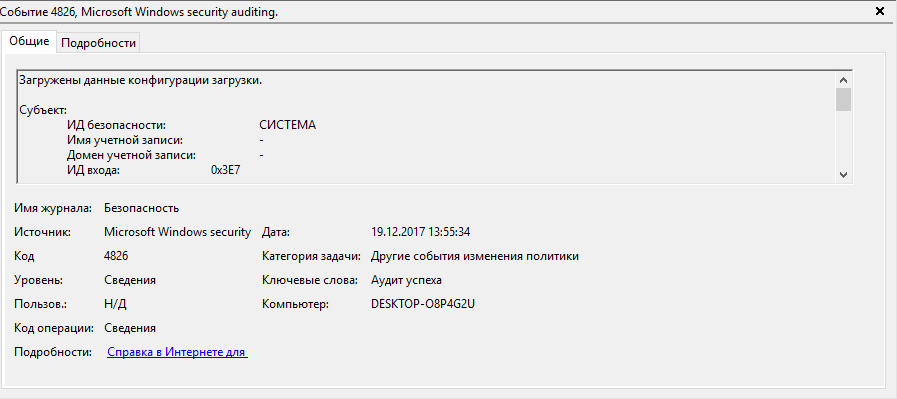
* Аудит доступа к объектам
* Аудит системных событий
* Аудит доступа к службе каталогов
* Аудит отслеживания процессов

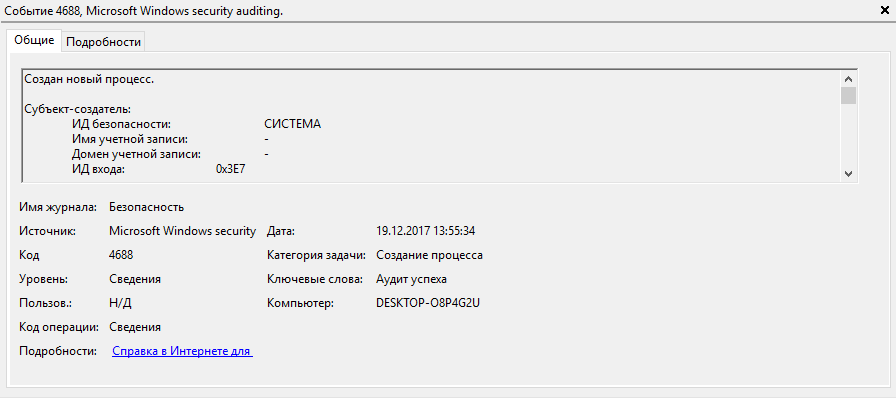
1. Включить в отчет о лабораторной работе копии экранных форм с краткой и полной информацией о просматриваемом событии безопасности.



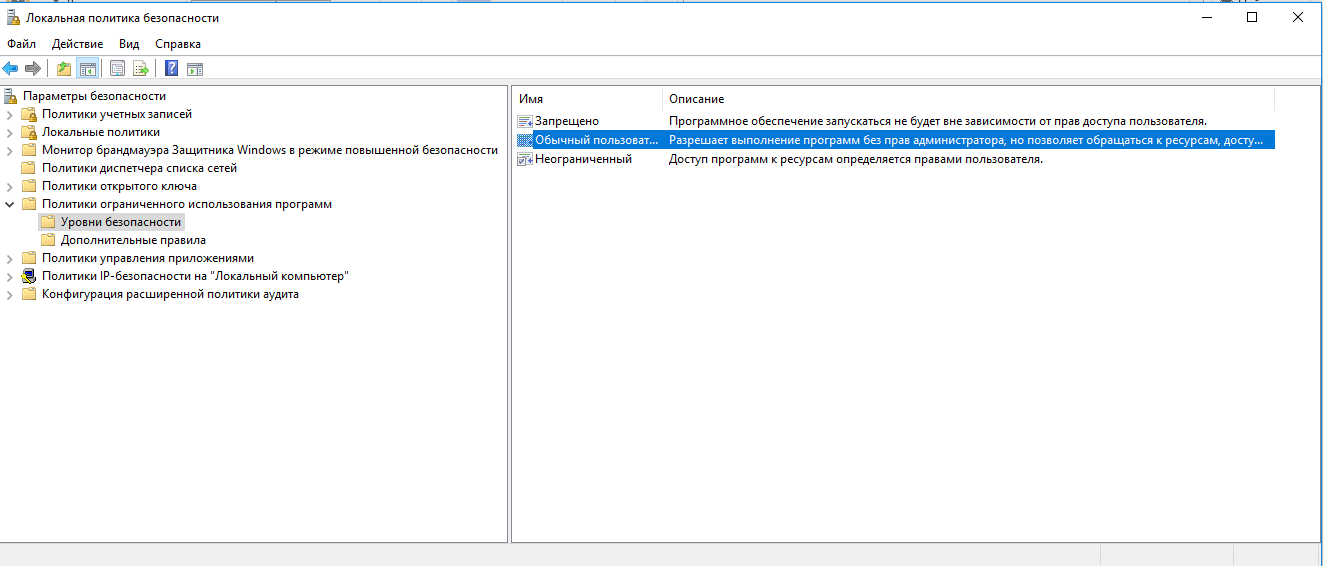


1. С помощью буфера обмена Windows и соответствующей кнопки в окне свойств события включить в отчет о лабораторной работе полную информацию о нескольких событиях безопасности.





1. Открыть окно определения уровней безопасности политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности).
2. Включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм.



* **Запрещено** - программное обеспечение запускаться не будет вне зависимости от прав доступа пользователя.
* **Обычный пользователь** - разрешает выполнение программ без прав администратора, но позволяет обращаться к ресурсам, доступным обычным пользователям.
* **Неограниченный** - доступ программ к ресурсам определяется правами пользователя.

1. В чем уязвимость с точки зрения безопасности информации принимаемая по умолчанию реакция системы на превышения размера журнала аудита?

*Когда журнал безопасности переполнится, Windows XP перестанет отвечать на запросы и будет выведено сообщение "Неудачная попытка аудита". Чтобы восстановить после остановки Windows XP, необходимо очистить журнал безопасности.*

1. Из каких этапов состоит построение политики безопасности для компьютерной системы?

* определение, какие данные и насколько серьезно необходимо защищать.
* определение кто и какой ущерб может нанести фирме в информационном аспекте.
* вычисление рисков и определение схемы уменьшения их до приемлемой величины.

1. К чему может привести ошибочное определение политики безопасности (приведите пример)?

*К потере/повреждению данных или системы.*

1. Почему, на ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

*На большинстве компьютеров подобные меры безопасности являются избыточными, а их настройка требует времени.*

1. Какие события безопасности должны фиксироваться в журнале аудита?

* Вход в систему
* Управление учетной записью
* Доступ к службе каталогов
* Доступ к объектам
* Изменения политики
* Использования привилегий
* Отслеживание процессов
* Системных событий
* Событий входа в систему

Журнал содержит в себе гигантское количество событий. Для анализа можно воспользоваться фильтрами или специальными утилитами.