Лабораторная работа 2

Управление политикой безопасности в операционной системе Windows

**Цель работы** - освоения средств администратора и аудитора операционной системы Windows.

1. Политика безопасностии аудит

**Политика безопасности** — это совокупность норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации.

**Аудит** — это процесс отслеживания действий пользователей и занесения выбранных типов событий в журнал безопасности. Политика аудита определяет типы событий, которые требуется собирать.

1. Журнал аудита

**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.

1. Цифровая подпись

**Цифровая подпись** — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа.

Вопросы:

1. Какие события безопасности должны фиксироваться в журнале аудита?

*В Журнале событий фиксируются следующие виды событий:*

* *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*

*Количество событий, которые записываются в журнал, очень велико, поэтому анализ журнала событий может быть довольно трудоемкой задачей. Для этого разработаны специальные утилиты, помогающие выявлять подозрительные события. Кроме того, можно фильтровать журнал по задаваемым критериям.*

1. Какие параметры определяют политику аудита?

* *Аудит вход в систему*
* *Аудит управление учетной записью*
* *Аудит доступ к службе каталогов*
* *Аудит доступ к объектам*
* *Аудит изменения политики*
* *Аудит использования привилегий*
* *Аудит отслеживание процессов*
* *Аудит системных событий*
* *Аудит событий входа в систему*

1. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

*Нет*

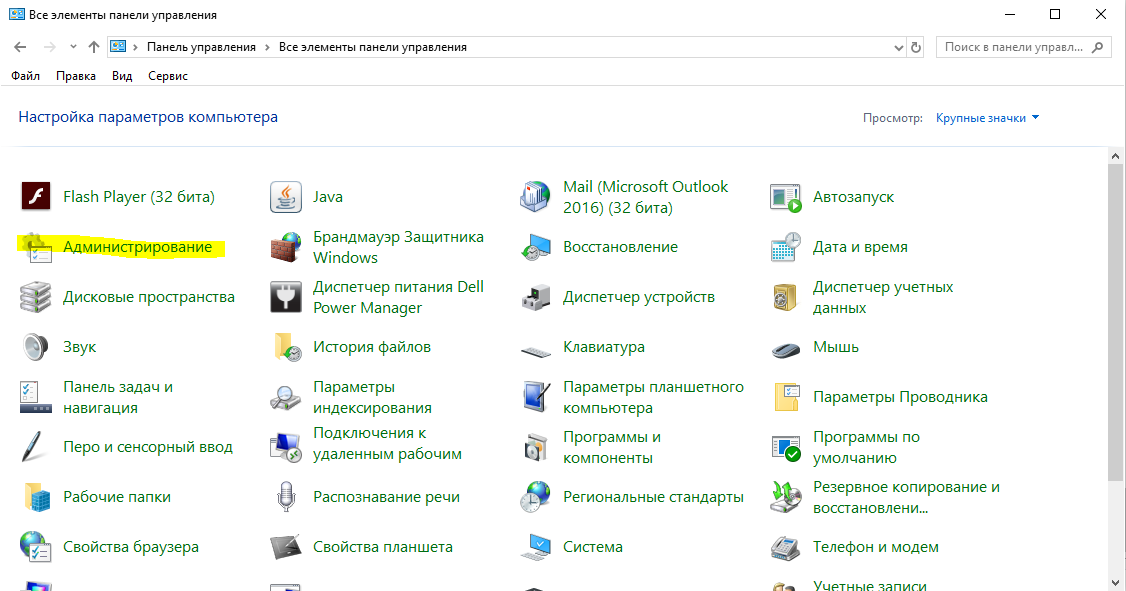
1. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя?

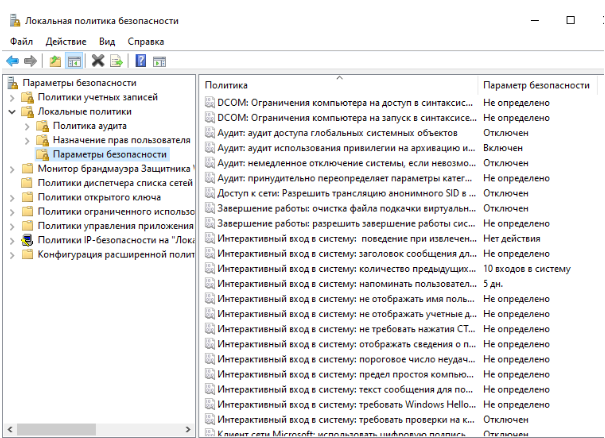
*В зашифрованном виде*

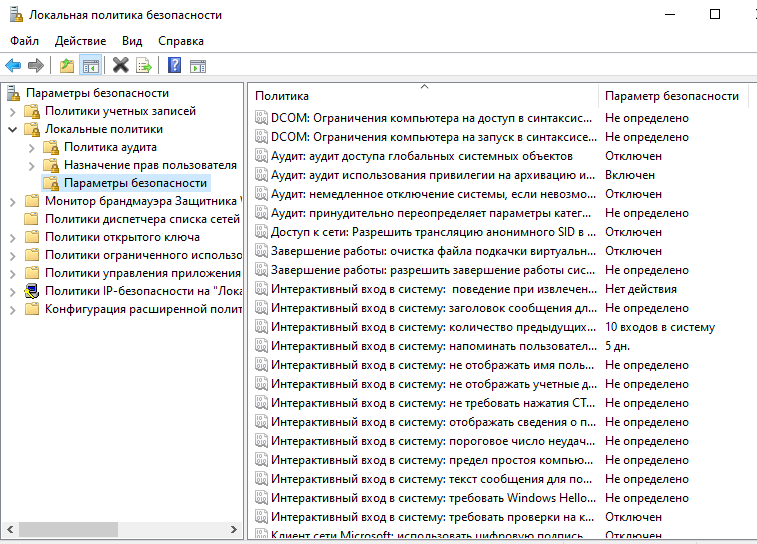
1. Нужно ли ограничивать права пользователей по запуску прикладных программ?

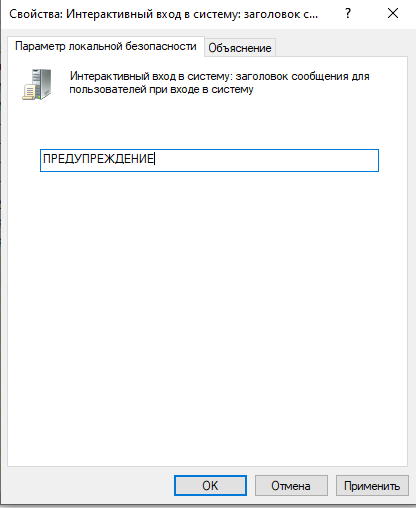
*Да*

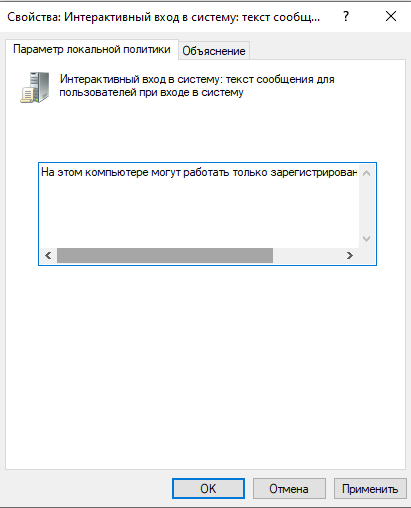
Ход работы:

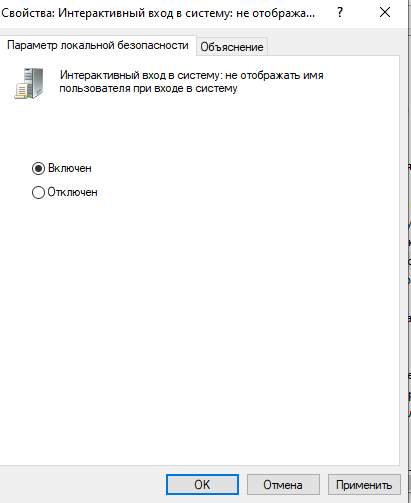


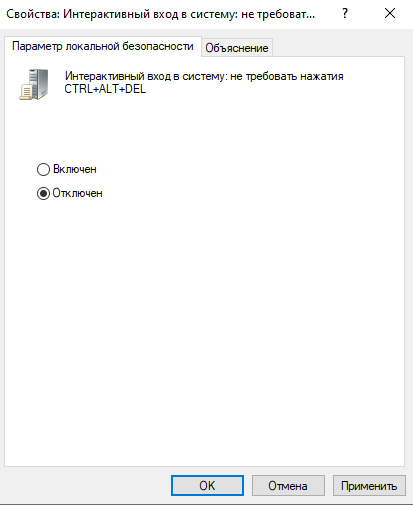


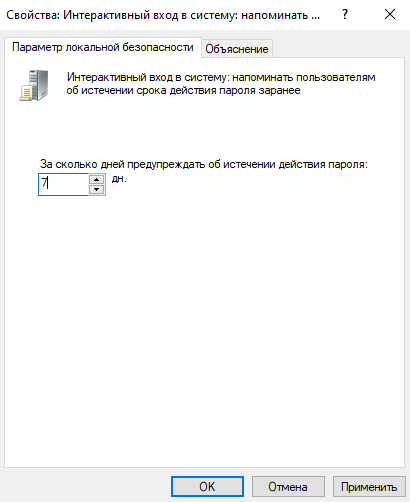


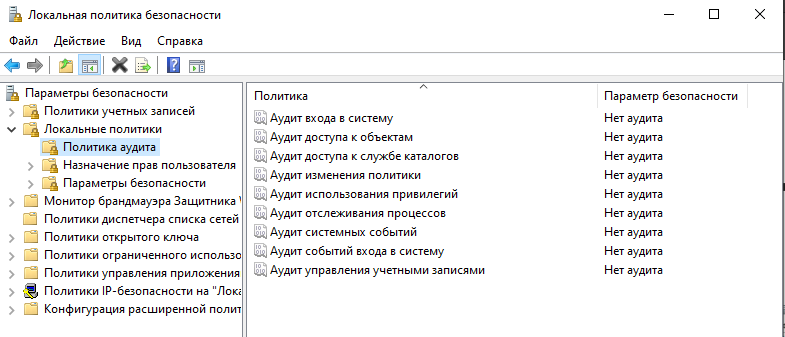


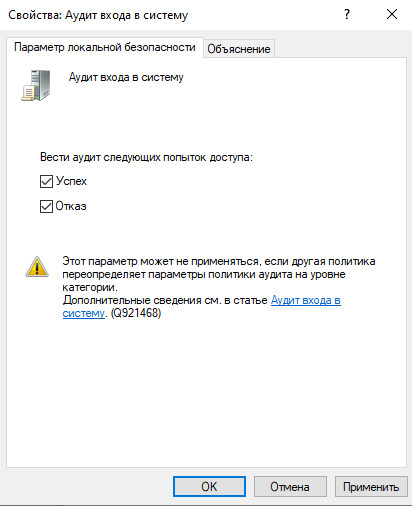


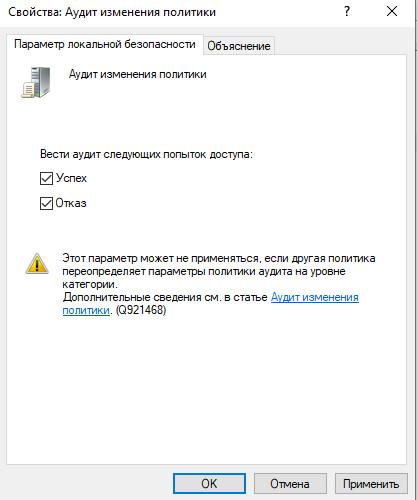


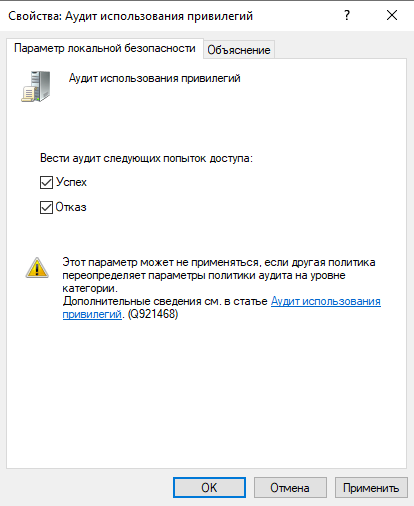


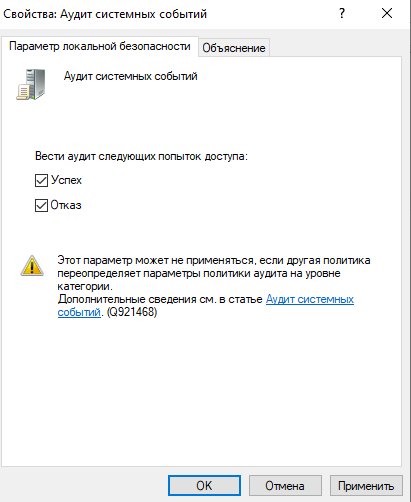


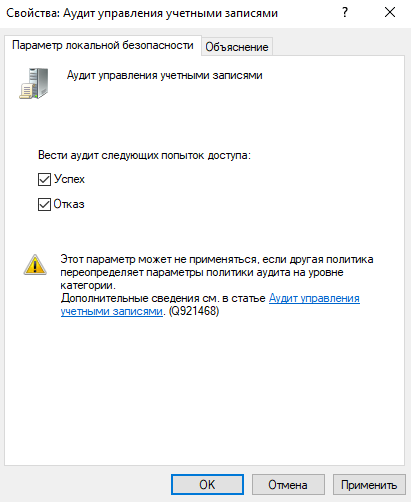


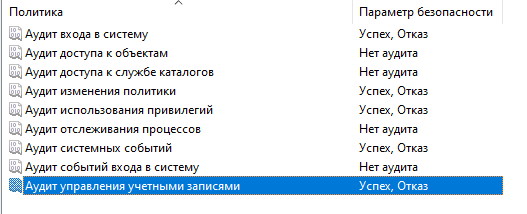


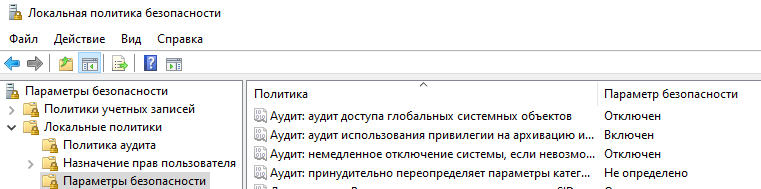


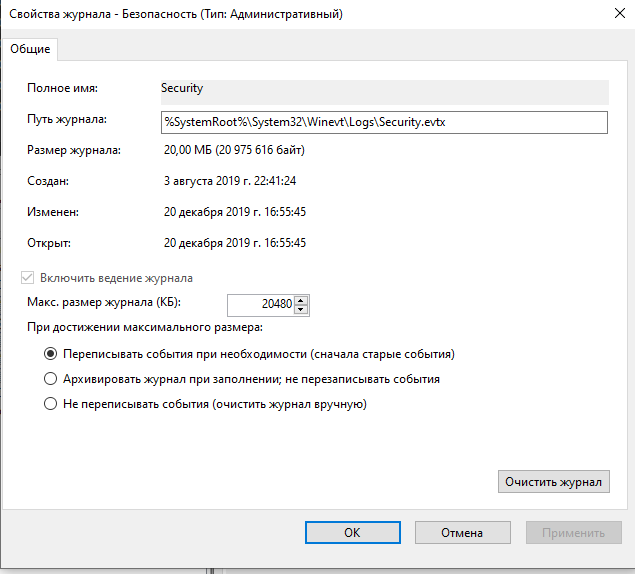


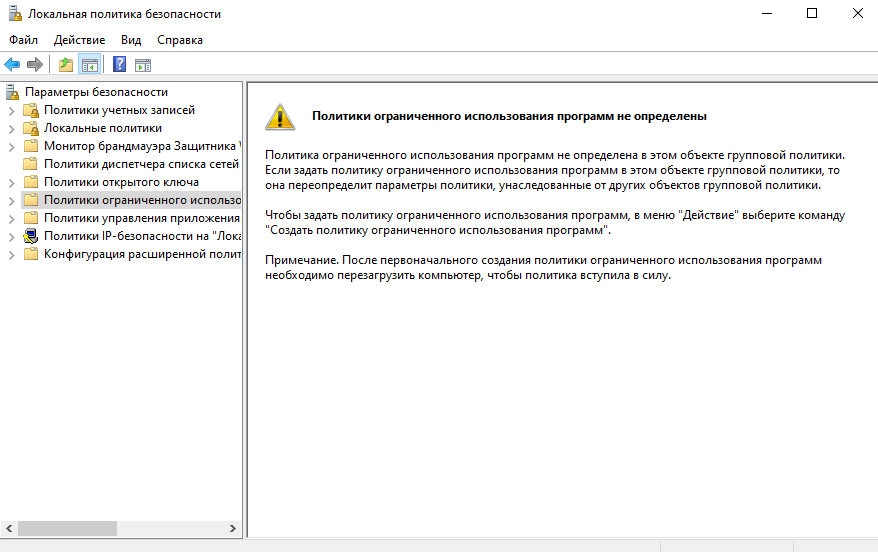


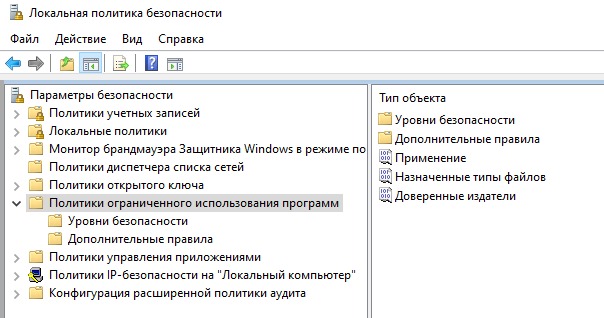


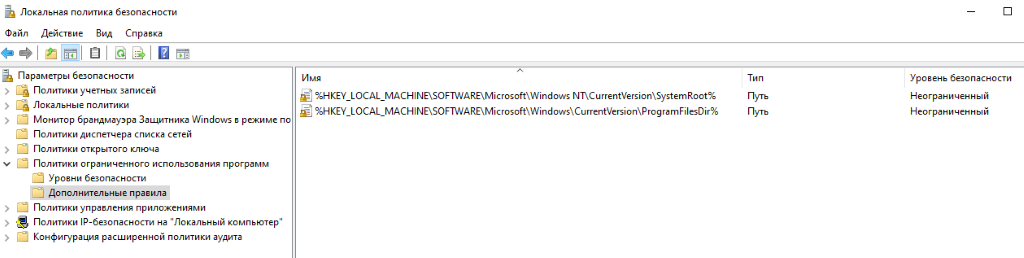












* Запрещено - программное обеспечение запускаться не будет вне зависимости от прав доступа пользователя.
* Обычный пользователь - разрешает выполнение программ без прав администратора, но позволяет обращаться к ресурсам, доступным обычным пользователям.
* Неограниченный - доступ программ к ресурсам определяется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

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.

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.

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

К потере/повреждению данных или системы.

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.

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.