Министерство науки и образования Украины

Харьковский национальный университет радиоэлектроники

Кафедра СТ

Отчет по лабораторной работе №3

Дисциплина: «Администрирование и сопровождение систем»

По теме: «Изучение особенностей сопровождения локальных политик безопасности»

|  |  |  |
| --- | --- | --- |
| Выполнили:  ст. гр. КН-15-1  Ткаченко Р.А.  Беляев Н.П.  Дмитриев А.В. |  | Принял:  Иванов В. Г. |

Харьков 2018

**Цель работы:** Научиться задавать политики безопасности учетных записей и назначение им соответствующие привилегий .

**Порядок выполнения заданий**

1. Освоить средства определения политики безопасности:
   * открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности);

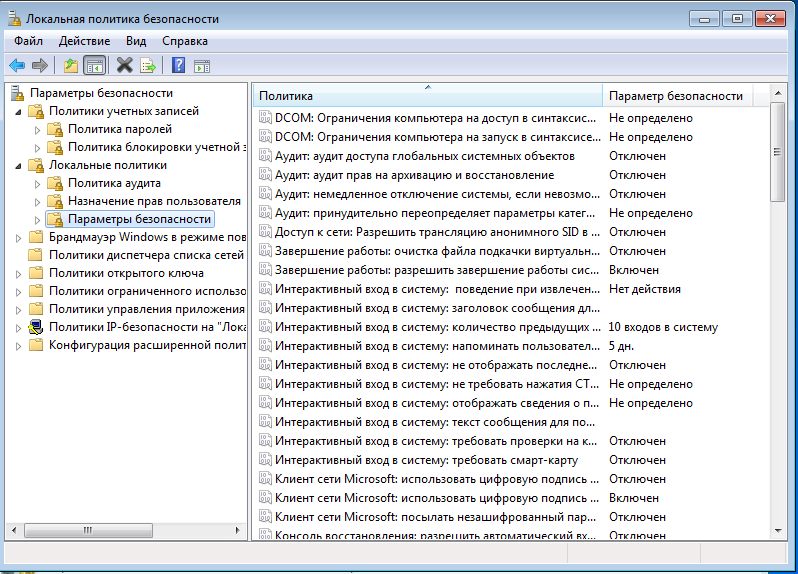


Рисунок 1

* + установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»;

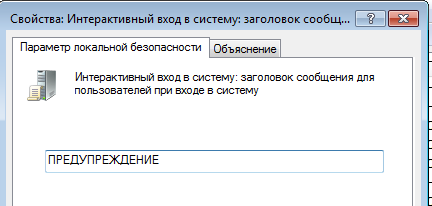


Рисунок 2

* + 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»;

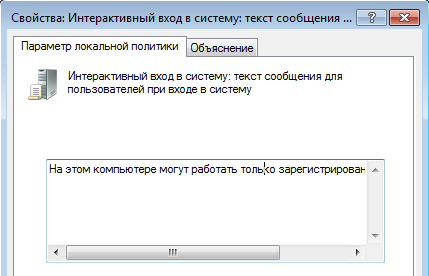


Рисунок 3

* + установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»;

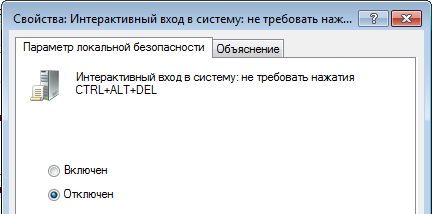


Рисунок 4

* + установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя»;

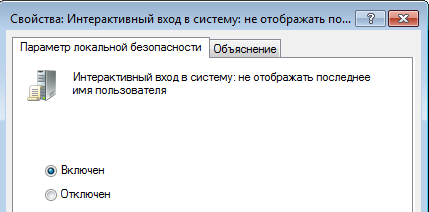


Рисунок 4

* + установить значение «7 дней» для параметра «Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее»; включить в отчет о лабораторной работе сведения о порядке назначения параметров политики безопасности, относящихся к интерактивному входу, и ответ на вопрос о смысле этих параметров;

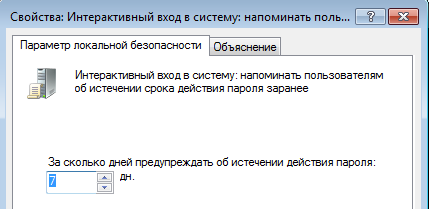


Рисунок 5

Освоить средства определение политики аудита:

* открыть окно определения параметров политики аудита (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Политика аудита);

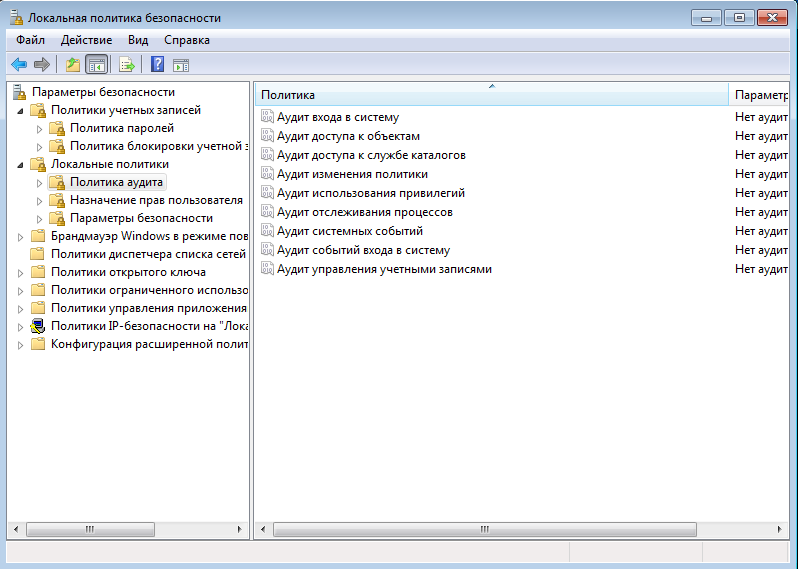


Рисунок 6

* 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;

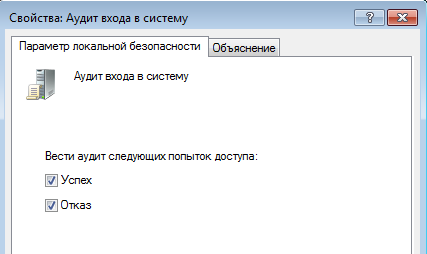


Рисунок 7

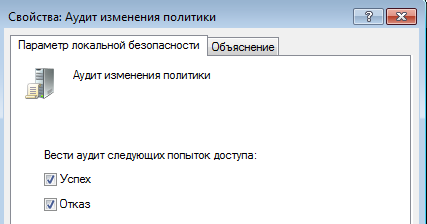


Рисунок 8

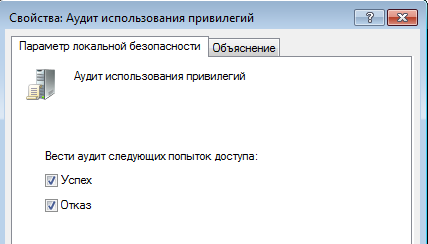


Рисунок 9

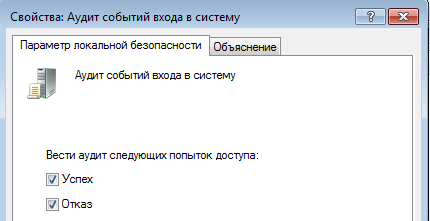


Рисунок 10

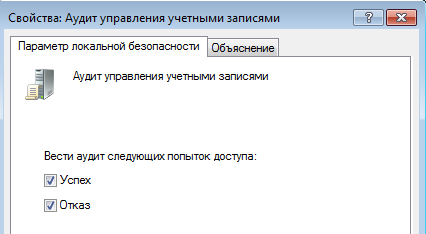
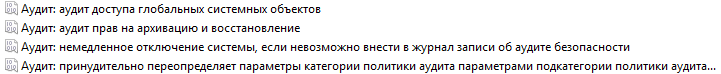


Рисунок 11

* открыть окно определения параметров безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности) и включить в отчет о лабораторной работе ответ на вопрос, какие еще параметры политики аудита могут быть определены;



* открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность), выполнить команду «Свойства» контекстного меню (или команду Действие | Свойства) и включить в отчет о лабораторной работе ответы на вопросы какие еще параметры политики аудита могут быть изменены, где расположен журнал аудита событий безопасности;

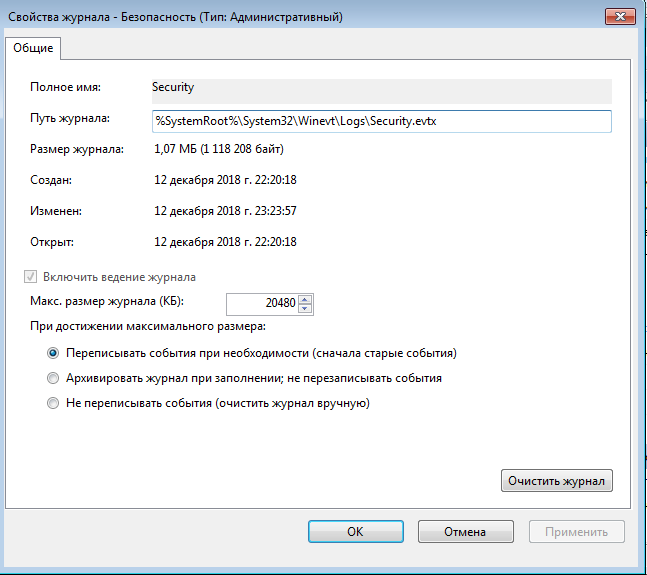


Рисунок 12

Освоить средства просмотра журнала аудита событий безопасности:

* включить в отчет о лабораторной работе копии экранных форм с краткой и полной информацией о просматриваемом событии безопасности;

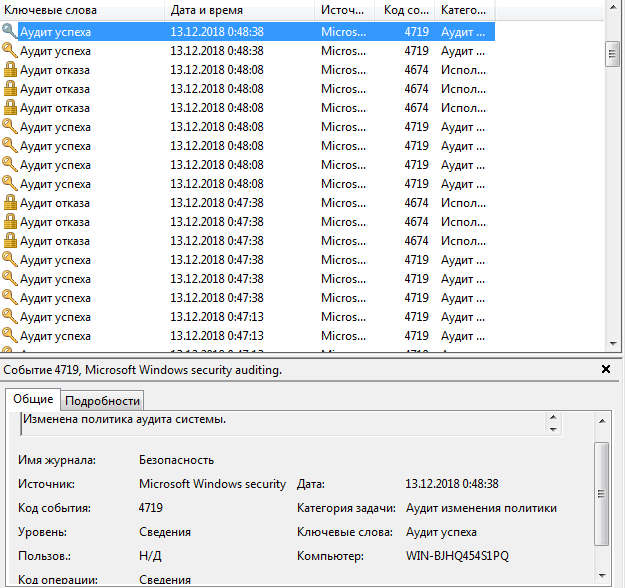


Рисунок 13

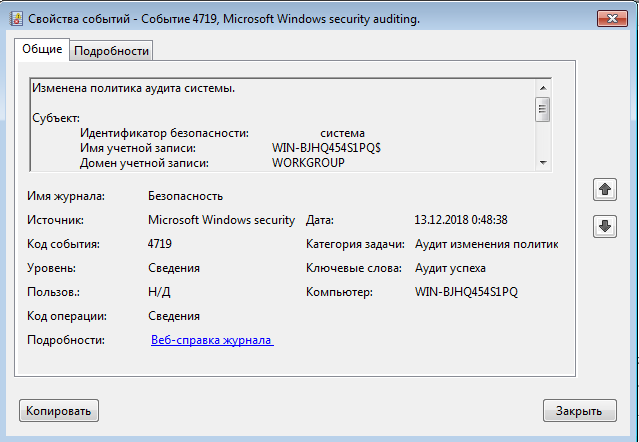


Рисунок 14

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

Имя журнала: Security

Источник: Microsoft-Windows-Security-Auditing

Дата: 13.12.2018 0:52:51

Код события: 4673

Категория задачи:Использование прав, затрагивающее конфиденциальные данные

Уровень: Сведения

Ключевые слова:Аудит успеха

Пользователь: Н/Д

Компьютер: WIN-BJHQ454S1PQ

Описание:

Вызвана привилегированная служба.

Субъект:

ИД безопасности: WIN-BJHQ454S1PQ\angel

Имя учетной записи: angel

Домен учетной записи: WIN-BJHQ454S1PQ

Код входа: 0x18ad3

Служба:

Сервер: Security

Имя службы: -

Процесс:

Идентификатор процесса: 0x488

Имя процесса: C:\Windows\System32\mmc.exe

Сведения о запросе службы:

Привилегии: SeCreateGlobalPrivilege

Xml события:

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">

<System>

<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />

<EventID>4673</EventID>

<Version>0</Version>

<Level>0</Level>

<Task>13056</Task>

<Opcode>0</Opcode>

<Keywords>0x8020000000000000</Keywords>

<TimeCreated SystemTime="2018-12-12T22:52:51.190308800Z" />

<EventRecordID>195</EventRecordID>

<Correlation />

<Execution ProcessID="512" ThreadID="532" />

<Channel>Security</Channel>

<Computer>WIN-BJHQ454S1PQ</Computer>

<Security />

</System>

<EventData>

<Data Name="SubjectUserSid">S-1-5-21-350528306-3773998320-2296719184-1000</Data>

<Data Name="SubjectUserName">angel</Data>

<Data Name="SubjectDomainName">WIN-BJHQ454S1PQ</Data>

<Data Name="SubjectLogonId">0x18ad3</Data>

<Data Name="ObjectServer">Security</Data>

<Data Name="Service">-</Data>

<Data Name="PrivilegeList">SeCreateGlobalPrivilege</Data>

<Data Name="ProcessId">0x488</Data>

<Data Name="ProcessName">C:\Windows\System32\mmc.exe</Data>

</EventData>

</Event>

Освоить средства определения политики ограниченного использования программ:

* открыть окно определения уровней безопасности политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности);

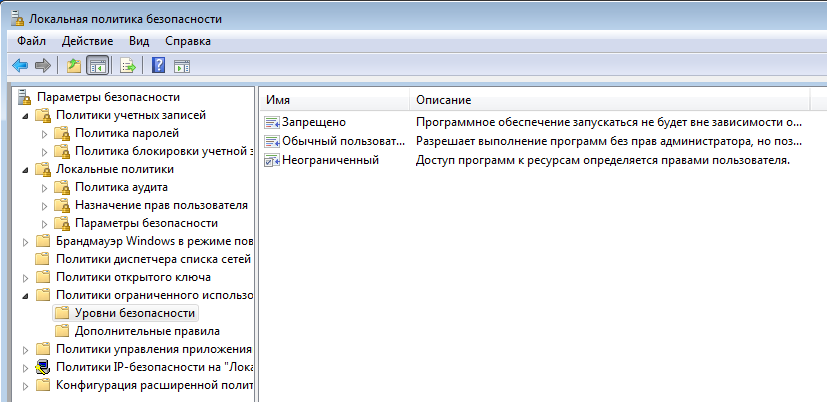


Рисунок 15

* включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм;

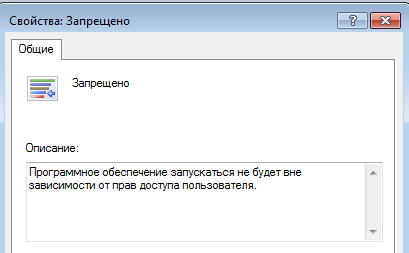


Рисунок 16

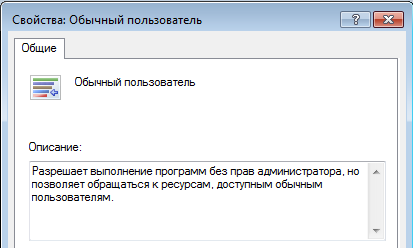


Рисунок 17

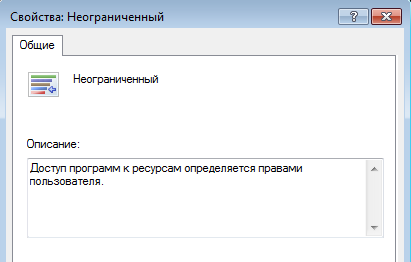


Рисунок 18

* открыть окно определения дополнительных правил политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Дополнительные правила);

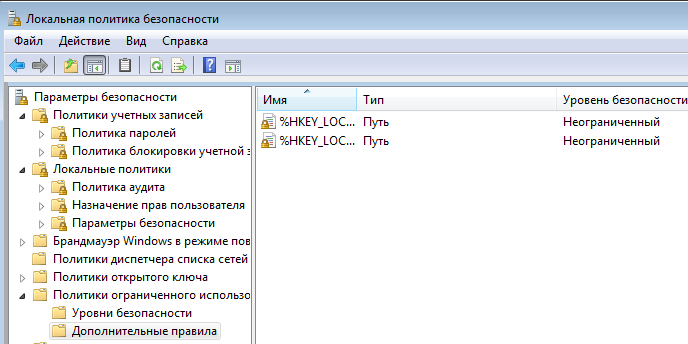


Рисунок 18

* включить в отчет о лабораторной работе ответы на вопросы, какие дополнительные правила для работы с программами могут быть определены (с помощью команд контекстного меню или меню «Действие») и в чем их смысл, а также копии соответствующих экранных форм.

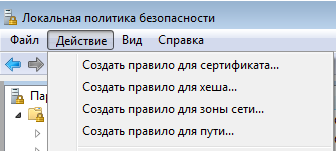


Рисунок 19

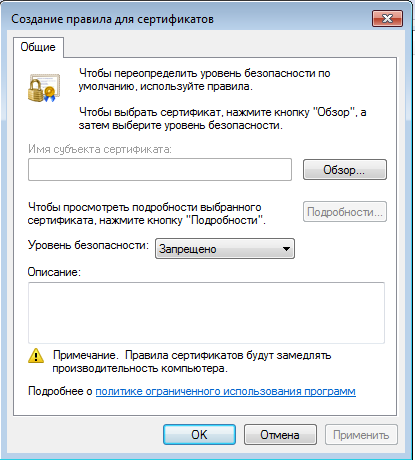


Рисунок 20

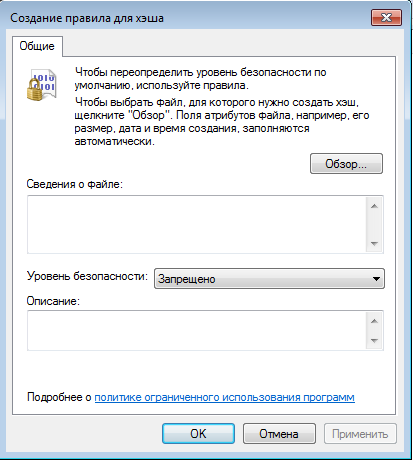


Рисунок 21

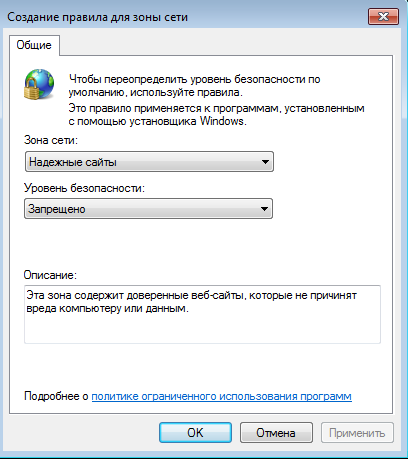


Рисунок 22

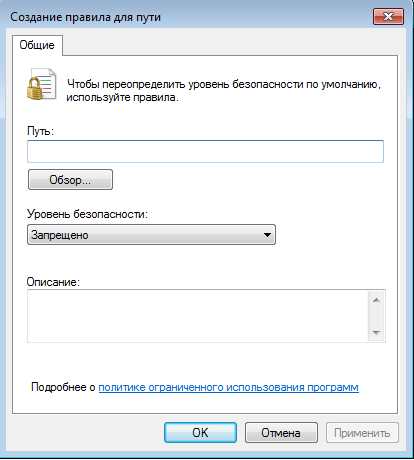


Рисунок 23

**Выводы:** при выполнения данной лабораторной работы были настроены локальные политики пользователей и политики аудита, был просмотрен журнал событий аудита. С помощью локальных политик можно гибко настраивать права и интерактивный вход пользователей организации, также с помощью политик можно повысить безопасность организации и уменьшить нагрузку IT персонала. С помощью политик аудита мы можем отслеживать как успешные так и неуспешные попытки входа в систему, изменения политики, доступа к объектам, использования привилегий и прочих. Это нам поможет вести отчетность о работе системы в организации и способствует ее улучшению.