МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ

ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

Кафедра «Информационные технологии»

И.Р. Усамов

Методические рекомендации к лабораторным работам по дисциплине «Теория информационных процессов и систем»

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль)

«Информационные системы и технологии»

«Информационные технологии в образовании»

«Информационные технологии в дизайне»

Квалификация

бакалавр

Грозный 20__

Составители:

Старший преподаватель кафедры
«Информационные технологии» Усамов И.Р.

Рецензент:

Э.Д. Алисултанова, доктор педагогических наук, кандидат физико-математических наук, профессор, директор Института прикладных информационных технологий, заведующая кафедрой «Информатика и вычислительная техника»

Методические указания предназначены для бакалавров по направлению подготовки 09.03.02 Информационные системы и технологии института прикладных информационных технологий.

Методические рекомендации рассмотрены и утверждены на заседании кафедры «Информационные технологии»: Протокол №__ от _____.20__г.

Рекомендовано к изданию редакционно-издательским советом ГГНТУ

СОДЕРЖАНИЕ

Введение

Цель курса заключается в изучении принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Курс закладывает набор базовых знаний, которые позволят выпускникам адаптироваться в условиях бурного развития информационных технологий. Обучение студентов данному курсу способствует воспитанию у них стремления к постоянному повышению профессиональной компетентности, расширению профессионального кругозора, умения ориентироваться в тенденциях и направлениях развития комплексной защиты информации.

Лабораторная работа №1 Разграничение прав пользователей

Определения понятий (изучить, включить в отчет):

- аутентификация,
- авторизация,
- администратор безопасности,
- симметричное и асимметричное шифрование,
- хеширование,
- политика безопасности.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) какие существуют способы аутентификации пользователей?
2) в чем слабость парольной аутентификации?
3) как может быть повышена надежность аутентификации с помощью паролей?
4) какой может быть реакция системы на попытку подбора паролей?
5) кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?
6) как должны храниться пароли в базе учетных записей пользователей?
7) в чем смысл объединения пользователей в группы?

Порядок выполнения работы:

1. Освоить средства регистрации пользователей

- открыть список зарегистрированных пользователей (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Пользователи);
- с помощью команды контекстного меню (Новый пользователь) создать для себя учетную запись с произвольным логическим именем;
- включить в отчет о лабораторной работе

1. копию экранной формы создания новой учетной записи,

2. копию экранной формы со списком зарегистрированных пользователей,

3. список команд контекстного меню (при отсутствии выделения имени пользователя в списке),

4. а также объяснения смысла четырех дополнительных параметров создаваемой учетной записи;

- выделить имя вновь зарегистрированного пользователя и с помощью команды контекстного меню (Свойства) просмотреть ее свойства;
- включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Общие» и объяснение разницы между отключением и блокировкой учетной записи;
- включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Членство в группах» и ответ на вопрос, в какую группу по умолчанию включается вновь созданный пользователь;
- с помощью кнопок «Добавить», «Дополнительно» и «Поиск» включить вновь созданного пользователя также в группу «Опытные пользователи»;
- включить в отчет о лабораторной работе копии экранных форм, используемых при добавлении пользователя в другую группу, и ответ на вопрос, как можно удалить пользователя из группы;
- включить в отчет о лабораторной работе список команд контекстного меню при выбранном имени учетной записи вместе с пояснениями их смысла, а также ответы на вопросы

1. когда должна применяться команда «Задать пароль»,
2. в чем опасность ее применения,
3. как должна происходить смена пароля пользователем.

2. Освоить средства работы с группами:

- открыть список групп (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Группы);

- включить в отчет сведения об автоматически создаваемых группах пользователей, их именах и характеристиках прав их членов;
- создать новую группу в системе с именем «Начинающие пользователи» и включить в отчет о лабораторной работе копию используемого при этом экрана и сведения о порядке создания в системе новых групп пользователей, а также ответ на вопрос, в чем целесообразность разбиения множества пользователей на группы.

3. Освоить порядок назначения прав пользователям:

- открыть окно настройки прав пользователей (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя);
- исключить группу пользователей «Все» из числа групп, обладающих правом «Доступ к компьютеру из сети»;
- исключить пользователя «Гость» из числа пользователей, обладающих правом «Локальный вход в систему»;
- добавить группу «Начинающие пользователи» к списку пользователей, обладающих правом «Локальный вход в систему»;
- включить в отчет о лабораторной работе копии экранов, используемых при назначении прав пользователям, и сведения о порядке выполнения этих действий;
- с помощью раздела справки Windows «Назначение прав пользователя» включить в отчет о лабораторной работе пояснения отдельных привилегий пользователей системы (в соответствии с номером варианта и приложением 1). Обязательно ответить на вопрос, почему использование данного права должно быть ограничено.

4. Освоить определение параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе:

- открыть окно определения параметров безопасности для паролей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей);
- включить в отчет о лабораторной работе сведения о порядке назначения максимального и минимального сроков действия паролей и ответ на вопрос о смысле подобных ограничений;
- включить в отчет о лабораторной работе сведения о порядке назначения минимальной длины и ограничений на сложность паролей, а также ответы на вопросы, какие и почему требования по сложности предъявляются к паролям в операционной системе Windows (с помощью справочной подсистемы);
- включить в отчет о лабораторной работе сведения о назначении параметров «Требовать неповторяемости паролей» и «Хранить пароли всех пользователей в домене, используя обратимое шифрование» (с помощью справки Windows);
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к паролям;
- открыть окно определения параметров безопасности для политики блокировки учетных записей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей);
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, и сведения о назначении этих параметров.

5. отчет о выполнение лабораторной работы должен включать в себя:

- титульный лист;
- содержание;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы.

Лабораторная работа №2 Реализация политики безопасности в защищенных версиях операционной системы Windows

Определение понятий (изучить, включить в отчет)

- *аудит*;
- *событие безопасности*;
- *журнал* (*файл*) *аудита*;
- *политика аудита*;
- *интерактивный вход*;
- *сетевой доступ*;
- *домен компьютерной сети*;
- *цифровая подпись*.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1) какие события безопасности должны фиксироваться в журнале аудита?

2) какие параметры определяют политику аудита?

3) целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?

4) целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

5) как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?

6) нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

Порядок выполнения работы:

1. Освоить средства определения политики безопасности:

- открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности);

- установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»;
- 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»;
- установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»;
- установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя»;
- 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;
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к интерактивному входу;
- с помощью раздела Справки Windows «Параметры безопасности» включить в отчет о лабораторной работе пояснения отдельных параметров локальной политики безопасности компьютерной системы и их возможных значений (в соответствии с номером варианта и приложением 1). Обязательно ответить на вопрос, чем может угрожать неправильное определение данного параметра.

2. Освоить средства определение политики аудита:

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

- 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;

- 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 | Администрирование | 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;

- включить в отчет о лабораторной работе сведения о порядке назначения параметров политики аудита и ответ на вопрос о смысле этих параметров;

- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики аудита.

3. Освоить средства просмотра журнала аудита событий безопасности:

- открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность);

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

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

4. 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);
- включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм;
- открыть окно определения дополнительных правил политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Дополнительные правила);
- 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.

5. отчет о выполнении лабораторной работы должен включать в себя:

- титульный лист
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы.

Лабораторная работа №3 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

подготовить для включения в отчет о лабораторной работе определения понятий

- *дискреционная политика безопасности*;
- *мандатная политика безопасности*;
- *субъект доступа*;
- *объект доступа*;
- *виды доступа*;
- *монитор обращений*;
- *монитор безопасности объектов*;
- *домен безопасности*;
- *реестр операционной системы*;
- *контроль целостности объектов*;
- *ключ симметричного шифрования*;
- *ключи асимметричного шифрования*.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

7) в чем достоинства и недостатки дискреционной политики безопасности?

8) в чем достоинства и недостатки мандатной политики безопасности?

9) в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?

10) кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?

11) каковы возможные пути нарушения политики безопасности в компьютерной системе?

12) какие факторы влияют на определение размеров доменов безопасности?

13) какая информация хранится в реестре Windows?

Порядок выполнения работы:

1. Освоить средства разграничения доступа пользователей к папкам:

- выполнить команду «Общий доступ и безопасность» контекстного меню папки, содержащей отчеты о выполненных лабораторных работах (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»;
- открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;
- с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);
- включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;
- открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;
- открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;
- закрыть окно дополнительных параметров безопасности и с помощью кнопки «Добавить» открыть окно выбора пользователя или группы;
- с помощью кнопок «Дополнительно» и «Поиск» открыть список зарегистрированных пользователей и групп и выбрать пользователя с именем своей индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- назначить ему права на полный доступ к папке с отчетами о выполненных лабораторных работах;
- включить в отчет копии экранных форм, использованных при выполнении заданий данного пункта.

3. Освоить средства разграничения доступа пользователей к файлам:

- выполнить команду «Свойства» контекстного меню файла с одним из отчетов о ранее выполненных лабораторных работах;

- повторить все задания п. 2, но применительно не к папке, а к файлу;
- включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам.

4. Освоить средства разграничения доступа к принтерам:

- выполнить команду «Принтеры и факсы» меню «Пуск»;
- выполнить команду «Свойства» контекстного меню установленного в системе принтера;
- повторить все задания п. 2, но применительно не к папке, а к принтеру (кроме добавления нового субъекта к списку управления доступом);
- включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам.

5. Освоить средства разграничения доступа к разделам реестра операционной системы:

- с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);
- с помощью команды «Разрешения» меню «Правка» редактора реестра определить и включить в отчет сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита (аналогично п. 2);
- включить в отчет копии экранных форм, использованных при выполнении данного пункта, и ответ на вопрос, в чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам.

6. Освоить средства обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы:

- выполнить команду «Свойства» контекстного меню папки, содержащей отчеты о ранее выполненных лабораторных работах, и на вкладке «Общие» окна свойств нажать кнопку «Другие»;

- включить выключатель «Шифровать содержимое для защиты данных», нажать кнопку «Применить» и в окне подтверждения изменения атрибутов нажать кнопку «Ok»;
- включить в отчет ответ на вопрос, как визуально выделяются имена зашифрованных файлов и папок;
- выполнить команду «Свойства» контекстного меню папки с отчетами о ранее выполненных лабораторных работах;
- нажать кнопку «Другие» и включить в отчет ответ на вопрос, доступна ли кнопка «Подробно»;
- повторить два предыдущих пункта для одного из файлов с отчетами о ранее выполненных лабораторных работах;
- выйти из системы и войти повторно под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- создать произвольный файл (например, с копией описания данной лабораторной работы) в папке «Мои документы» и обеспечить шифрование этого файла;
- выйти из системы и снова войти под именем общей учетной записи, под которой работали первоначально;
- выполнить команду «Свойства» контекстного меню одного из файлов с отчетами о ранее выполненных лабораторных работах, нажать последовательно кнопки «Другие» и «Подробно»;
- в окне подробностей шифрования нажать кнопку «Добавить» и в окне выбора пользователя выбрать имя индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- повторить два предыдущих пункта для всех файлов с отчетами о ранее выполненных работах;
- снова выйти из системы и войти повторно под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;

•убедиться, что под индивидуальной учетной записью можно просматривать и редактировать отчеты о ранее выполненных лабораторных работах;

•включить в отчет копии экранных форм, использованных при выполнении данного пункта, сведения о порядке использования шифрующей файловой системы и ответы на вопросы

♦ как формируется список пользователей, из которого возможен выбор субъектов для совместного доступа к зашифрованным файлам;

♦ связан ли этот список с зарегистрированными в системе пользователями и группами;

♦ каковы функции агента восстановления зашифрованных файлов и как он может быть назначен (воспользуйтесь Справкой Windows).

7. Ознакомиться с правами доступа к файлам и папкам, назначаемым операционной системой по умолчанию:

•выполнить команду «Общий доступ и безопасность» (команду «Свойства») контекстного меню одной из папок с документами зарегистрированного в системе пользователя (например, «Документы - Пользователь компьютерного класса») и открыть вкладку «Безопасность»;

•включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце;

•повторить два предыдущих пункта для папки с документами другого зарегистрированного пользователя;

•повторить два предыдущих пункта для папки «Общие документы»;

•включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и ответы на вопросы

♦ как обеспечивается операционной системой разграничение доступа к личным документам пользователей (по умолчанию);

♦ где (по умолчанию) должны находиться документы, предназначенные для совместного использования.

9. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы.

Лабораторная работа № 4 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7

подготовить для включения в отчет о лабораторной работе определения понятий

- *матрица доступа*;
- *дискреционный список контроля доступа*;
- *домен безопасности*;
- *журнал (файл) аудита*;
- *запись журнала аудита*;
- *стандарт безопасности*.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

14) что такое Trusted Computer System Evaluation Criteria (TCSEC)?

15) какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?

16) какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?

17) кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?

18) как должны использоваться записи журнала аудита событий безопасности?

19) какие права доступа к файлу аудита имеет по умолчанию администратор системы?

20) что такое консольное приложение Windows?

Порядок выполнения работы:

2. Освоить использование системной программы по управлению списками контроля доступа (CACLS):

- начать сеанс работы в режиме командной строки Windows (Пуск | Программы | Стандартные | Командная строка);
- в строке приглашения ввести название программы, ознакомиться с ее назначением и параметрами и сохранить данную информацию в отчете о лабораторной работе (через буфер обмена с помощью команд подменю «Изменить» системного меню окна командной строки);
- перейти (с помощью команды cd имя папки) в индивидуальную папку и с помощью программы cacls получить и сохранить в файле в своей индивидуальной папке разрешения на доступ к папке с лабораторными работами, введя следующую команду

cacls имя папки с лаб.работами >*имя файла*

(для переключения раскладок клавиатуры в режиме командной строки использовать комбинации клавиш Alt+правый Shift и Alt+левый Shift);

- просмотреть созданный файл с помощью Internet Explorer и включить его содержимое в отчет о лабораторной работе, снабдив необходимыми комментариями (с учетом сведений, приведенных в приложении);
- перейти в свою индивидуальную папку (с помощью команды командной строки cd) и с помощью одного вызова программы cacls запретить доступ группе «Пользователи» ко всем файлам и вложенным папкам своей индивидуальной папки;
- проверить результаты выполнения предыдущего пункта с помощью команды «Свойства» контекстного меню своей индивидуальной папки и включить в отчет о лабораторной работе текст вызова программы cacls и ответ на вопрос, почему доступ Вам к файлам своей папки теперь недоступен;

- разрешить доступ по чтению группе «Пользователи» к файлам и вложенным папкам своей индивидуальной папки с помощью одного вызова программы cacls, проверить результаты и включить в отчет о лабораторной работе текст вызова программы cacls;

- завершить (с помощью команды exit) сеанс работы в режиме командной строки и включить в отчет о лабораторной работе ответ на вопрос, в чем преимущество использования программы cacls перед назначением разрешений на доступ к объектам при помощи Проводника Windows.

3. Изучить средства эффективного анализа журнала аудита событий безопасности:

- начать работу с системной программой Просмотр событий (Панель управления | Администрирование) и открыть журнал аудита событий безопасности;

- с помощью команды «Фильтр» меню «Вид» изучить и отразить в отчете о лабораторной работе средства отбора необходимых для анализа записей (критерии отбора, переход от просмотра отобранных записей к просмотру всего журнала и наоборот, изменение порядка сортировки записей, поиск нужных записей, изменение вида отображения записей);

- с помощью команд меню «Действие» изучить и отразить в отчете средства сохранения и восстановления журнала аудита (сохранить журнал аудита событий безопасности в виде текстового файла в своей индивидуальной папке);

- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и завершить работу с системной программой Просмотр событий;

3. Ознакомиться с возможностями системной программы дополнительной защиты базы учетных записей с помощью ее шифрования:

- начать работу с программой syskey с помощью команды «Выполнить» меню «Пуск»;

- нажать кнопку «Обновить», ознакомиться и отразить в отчете варианты генерации системного ключа шифрования базы учетных записей, нажать кнопку «Отмена» (дважды);
- включить в отчет о лабораторной работе ответ на вопрос, какие достоинства и недостатки есть у каждого из предлагаемых программой syskey вариантов генерации криптографического ключа.

4. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

- почему компьютерные системы на основе Windows XP не могут быть сертифицированы по классу безопасности TCSEC выше, чем C2?
- какой класс защищенности автоматизированных систем в соответствии с требованиями руководящих документов Гостехкомиссии РФ соответствует, на Ваш взгляд, классу C2 TCSEC?
- какие угрозы безопасности и каналы утечки конфиденциальной информации может устранить программа syskey?

9. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;

Приложение

Стандартные типы доступа к объектам в операционной системе Windows XP

- SINCHRONIZE – использовать объект для синхронизации;
- WRITE_OWNER – изменить владельца объекта;
- WRITE_DAC – изменить дискреционный список контроля доступа к объекту;

- READ_CONTROL – прочитать данные из дискреционного списка контроля доступа;
- DELETE – удалить объект.

Специальные права доступа к объектам

- READ_DATA – прочитать данные из объекта;
- WRITE_DATA – записать данные в объект;
- APPEND_DATA – добавить данные в объект;
- READ_ATTRIBUTES – прочитать атрибуты объекта;
- WRITE_ATTRIBUTES – записать атрибуты объекта;
- READ_EA – прочитать расширенные атрибуты объекта;
- WRITE_EA – записать расширенные атрибуты объекта;
- EXECUTE – выполнить программный файл.

Родовые права доступа к объектам

- GENERIC_READ - READ_CONTROL, READ_DATA, READ_ATTRIBUTES, READ_EA, SINCHRONIZE;
- GENERIC_WRITE - READ_CONTROL, WRITE_DATA, WRITE_ATTRIBUTES, WRITE_EA, APPEND_DATA, SINCHRONIZE;
- GENERIC_EXECUTE - READ_CONTROL, READ_ATTRIBUTES, EXECUTE, SINCHRONIZE.

Лабораторная работа № 5 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP

Цель работы: освоение системных программ Windows XP, программ из комплекта Windows NT Resource Kit и других программных средств, предназначенных для

- просмотра и управления разрешениями на доступ к конфиденциальным объектам компьютерной системы;
- просмотра и анализа записей аудита;

- анализа соответствия реализуемой в компьютерной системе политики безопасности требованиям стандартов безопасности;
- дополнительной защиты базы учетных записей пользователей компьютерной системы и используемых ими рабочих станций.

Подготовка к выполнению работы: по материалам лекций по дисциплине «Защита информационных процессов в компьютерных системах» и изученным ранее дисциплинам («Введение в специальность», «Теория информационной безопасности и методология защиты информации» и другим) вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

- *матрица доступа*;
- *дискреционный список контроля доступа*;
- *домен безопасности*;
- *журнал (файл) аудита*;
- *запись журнала аудита*;
- *стандарт безопасности*.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

21) что такое Trusted Computer System Evaluation Criteria (TCSEC)?

22) какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?

23) какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?

24) кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?

25) как должны использоваться записи журнала аудита событий безопасности?

26) какие права доступа к файлу аудита имеет по умолчанию администратор системы?

27) что такое консольное приложение Windows?

Порядок выполнения работы:

4. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами администратора).

5. Освоить использование системной программы по управлению списками контроля доступа (CACLS):

- начать сеанс работы в режиме командной строки Windows XP (Пуск | Программы | Стандартные | Командная строка);
- в строке приглашения ввести название программы, ознакомиться с ее назначением и параметрами и сохранить данную информацию в отчете о лабораторной работе (через буфер обмена с помощью команд подменю «Изменить» системного меню окна командной строки);
- перейти (с помощью команды cd \Учебные материалы) в папку «Учебные материалы» и с помощью программы cacls получить и сохранить в файле в своей индивидуальной папке разрешения на доступ к папке «КЗИ2000», введя следующую команду

cacls КЗИ2000 >*имя файла*

(для переключения раскладок клавиатуры в режиме командной строки использовать комбинации клавиш Alt+правый Shift и Alt+левый Shift);

- просмотреть созданный файл с помощью Internet Explorer и включить его содержимое в отчет о лабораторной работе, снабдив необходимыми комментариями (с учетом сведений, приведенных в приложении);
- повторить два предыдущих пункта для своей индивидуальной папки;
- перейти в свою индивидуальную папку (с помощью команды командной строки cd) и с помощью одного вызова программы cacls запретить доступ группе «Пользователи» ко всем файлам и вложенным папкам своей индивидуальной папки;
- проверить результаты выполнения предыдущего пункта с помощью команды «Свойства» контекстного меню своей индивидуальной папки и

включить в отчет о лабораторной работе текст вызова программы cacls и ответ на вопрос, почему доступ Вам к файлам своей папки теперь недоступен;

- разрешить доступ по чтению группе «Пользователи» к файлам и вложенным папкам своей индивидуальной папки с помощью одного вызова программы cacls, проверить результаты и включить в отчет о лабораторной работе текст вызова программы cacls;
- завершить (с помощью команды exit) сеанс работы в режиме командной строки и включить в отчет о лабораторной работе ответ на вопрос, в чем преимущество использования программы cacls перед назначением разрешений на доступ к объектам при помощи Проводника Windows.

6. Ознакомиться с возможностями программ управления и анализа разрешений на доступ к объектам компьютерных систем на основе Windows XP:

- начать работу с программой просмотра разрешений на доступ к объектам и параметров политики безопасности DumpACL, размещенной в папке TEMP \ DumpACL на диске c;
- ознакомиться с порядком настройки параметров отчета о результатах анализа разрешений (команда меню Report | Permissions Report Options) и включить эти сведения в отчет о лабораторной работе;
- с помощью команды меню Report | Dump Permissions for File System получить и включить в отчет сведения о результатах анализа разрешений на доступ к папке «КЗИ2000» и своей индивидуальной папке, а также ответ на вопрос, в чем разница между данными результатами и сведениями, полученными при помощи команды cacls;
- с помощью других команд меню Report получить и включить в отчет результаты анализа разрешений на доступ к реестру Windows (только раздел HKEY_CURRENT_USER) и принтеру;
- ознакомиться и включить в отчет о лабораторной работе сведения о порядке получения и содержании информации о зарегистрированных пользователях и группах (команды Dump… меню Report);

- включить в отчет о лабораторной работе сведения о назначении и результатах применения команд Dump Policies и Dump Rights меню Report;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой DumpACL, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к объектам FileAdmin из группы Administrator Assistant меню Пуск | Программы;
- получить с помощью данной программы разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке и включить их в отчет;
- с помощью программы FileAdmin оставить полный доступ к своей индивидуальной папке, вложенным в нее папкам и файлам только самому себе (своей индивидуальной учетной записи) и пользователю User (учесть при этом действие переключателей “Propagate Through Entire Tree?”), а всем остальным пользователям и группам – доступ только для чтения;
- с помощью программы FileAdmin (кнопка Clone) распространить виды доступа к своей индивидуальной папке, установленные для группы «Пользователи», на группу «Опытные пользователи»;
- изучить назначение кнопки Options программы FileAdmin (определение настроек и просмотр журнала изменений прав доступа к объектам);
- включить в отчет о лабораторной работе копии экранных форм, используемых программой FileAdmin, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к реестру Windows RegAdmin из группы Administrator Assistant меню Пуск | Программы;
- с помощью программы RegAdmin получить и включить в отчет о лабораторной работе сведения о разрешениях на доступ к разделам реестра HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER, а также ответ на вопрос, как изменить права доступа к разделам реестра Windows с помощью программы RegAdmin;

- включить в отчет о лабораторной работе копии экранных форм, используемых программой RegAdmin, и завершить работу с этой программой;
- начать работу с программой управления и анализа разрешений на доступ к объектам Security Explorer из группы Administrative Tools (Common) меню Пуск | Программы;
- с помощью программы Security Explorer (команда меню Tools | Show permissions) просмотреть и включить в отчет о лабораторной работе разрешения на доступ к папке «КЗИ2000» и к своей индивидуальной папке, а также ответ на вопрос, какая дополнительная информация о дискреционных списках контроля доступа выводится программой Security Explorer;
- изучить и включить в отчет сведения о назначении кнопок диалогового окна Directory Permissions программы Security Explorer (Modify, Grant Permissions и т.д.), а также ответ на вопрос, возможно ли «клонирование» прав доступа к объекту в программе Security Explorer;
- с помощью команды меню Tools | Search for Permissions программы Security Explorer получить, сохранить в файле в своей индивидуальной папке и включить в отчет о лабораторной работе сведения о папках диска с, к которым имеет доступ (в том числе полный) группы «Пользователи» и «Все»;
- изучить и отразить в отчете о лабораторной работе средства вызова функций программы Security Explorer с помощью контекстного меню Проводника Windows;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой Security Explorer, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к объектам Security Manager из группы Admin Tools меню Пуск | Программы;
- получить с помощью программы Security Manager и включить в отчет о лабораторной работе разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке (для сохранения отчета программы можно воспользоваться командой ее меню File | Save Report);

- выделить в левой части окна программы Security Manager имя своей индивидуальной папки и на ее примере изучить и включить в отчет о лабораторной работе команды контекстного меню и связанные с ними функции этой программы по управлению разрешениями на доступ к объектам (особо обратить внимание на команду Replace Owner и включить в отчет о лабораторной работе ответ на вопрос, в чем потенциальная опасность применения этой возможности);
- включить в отчет о лабораторной работе копии экранных форм, используемых программой Security Manager, и завершить работу с этой программой;
- начать работу с программой управления разрешениями на доступ к объектам компьютерной системы предприятия Virtuosity (с помощью меню Пуск | Программы);
- с помощью программы Virtuosity получить и отразить в отчете разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке;
- с помощью Справки программы Virtuosity изучить и включить в отчет о лабораторной работе сведения о назначении команд меню Actions | Save into Database и Actions | Apply from Database;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой Virtuosity, и завершить работу с этой программой.

7. Ознакомиться с возможностями программ анализа выбранной для компьютерной системы политики безопасности и ее соответствия требованиям стандартов в области информационной безопасности:

- начать работу с программой проверки соответствия настроек Windows XP требованиям класса C2 TCSEC (программа c2config из комплекта Windows NT Resource Kit) с помощью команды «Выполнить» меню «Пуск»;
- ознакомиться с результатами анализа политики безопасности, полученными с помощью программы c2config, сохранить их в отчете о лабораторной работе и снабдить необходимыми комментариями, раскрывающими сущность того или иного анализируемого параметра

(наиболее подробно для тех параметров, значения которых не соответствуют требованиям класса безопасности C2);

- включить в отчет сведения о смысле изображений рядом с анализируемым параметром политики безопасности в окне программы c2config (при необходимости можно воспользоваться разделом List Box Display Справки данной программы;
- включить в отчет о лабораторной работе копии экранных форм, используемых программой c2config, и завершить работу с этой программой;
- начать работу с демонстрационной версией программы анализа безопасности компьютерных систем и сетей Kane Security Analyst из группы Kane Security Analyst for NT меню Пуск | Программы;
- с помощью кнопок главного окна программы Kane Security Analyst изучить и включить в отчет ее основные функции (анализ политики учетных записей, выбираемых пользователями паролей, политики аудита, прав доступа к файлам и папкам, прав доступа к реестру, соответствия требованиям класса C2, рисков при использовании данной политики безопасности и др.);
- включить в отчет о лабораторной работе копии экранных форм, используемых программой Kane Security Analyst, и завершить работу с этой программой.

8. Изучить средства эффективного анализа журнала аудита событий безопасности:

- начать работу с системной программой Просмотр событий (Панель управления | Администрирование) и открыть журнал аудита событий безопасности;
- с помощью команды «Фильтр» меню «Вид» изучить и отразить в отчете о лабораторной работе средства отбора необходимых для анализа записей (критерии отбора, переход от просмотра отобранных записей к просмотру всего журнала и наоборот, изменение порядка сортировки записей, поиск нужных записей, изменение вида отображения записей);

- с помощью команд меню «Действие» изучить и отразить в отчете средства сохранения и восстановления журнала аудита (сохранить журнал аудита событий безопасности в виде текстового файла в своей индивидуальной папке);
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и завершить работу с системной программой Просмотр событий;
- запустить в режиме командной строки программу dumpel из комплекта Windows NT Resource Kit с параметром -?, включить в отчет сведения о параметрах этой программы работы с журналами аудита;
- с помощью программы dumpel сохранить в текстовом файле в своей индивидуальной папке выбранные записи системного журнала аудита, введя следующую строку

dumpel –l system –f *имя файла* –e 6005 –e 6006 –e 6009 –m EventLog

Включить в отчет фрагмент созданного таким образом файла и ответ на вопрос, какая дополнительная по сравнению с системной программой Просмотр событий возможность существует у программы dumpel;

- завершить работу в режиме командной строки.

6. Ознакомиться с возможностями системной программы дополнительной защиты базы учетных записей с помощью ее шифрования:

- начать работу с программой syskey с помощью команды «Выполнить» меню «Пуск»;
- нажать кнопку «Обновить», ознакомиться и отразить в отчете варианты генерации системного ключа шифрования базы учетных записей, нажать кнопку «Отмена» (дважды);
- включить в отчет о лабораторной работе ответ на вопрос, какие достоинства и недостатки есть у каждого из предлагаемых программой syskey вариантов генерации криптографического ключа.

7. Ознакомиться с возможностями дополнительного хранителя экрана из комплекта Windows NT Resource Kit, осуществляющего принудительный выход из системы по истечении заданного периода времени:

- скопировать файл winexit.scr из папки C:\Disrtrib\Resource Kit 2\COMMON\COMMON в папку C:\WINDOWS\system32 (если это еще не сделано);
- с помощью команды «Свойства» контекстного меню Рабочего стола (закладка «Заставка») установить и настроить (кнопка «Параметры») хранитель экрана Logoff Screen Saver;
- закрыть окно свойств экрана и проверить работу установленного хранителя экрана;
- включить в отчет о лабораторной работе сведения о параметрах и порядке использования дополнительного хранителя экрана, а также копии экранных форм, использованных при выполнении данного пункта.

8. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

- почему компьютерные системы на основе Windows XP не могут быть сертифицированы по классу безопасности TCSEC выше, чем C2?
- какой класс защищенности автоматизированных систем в соответствии с требованиями руководящих документов Гостехкомиссии РФ соответствует, на Ваш взгляд, классу C2 TCSEC?
- почему многие из рассмотренных в настоящей лабораторной работе программ работают в режиме командной строки?
- какая из рассмотренных в данной лабораторной работе программ управления разрешениями на доступ к объектам кажется Вам наиболее удобной и почему?
- составьте строку вызова системной программы cacls для того, чтобы обеспечить доступ по чтению ко всем файлам и папкам папки c:\students для всех членов группы «Преподаватели»;

- в чем преимущества, на Ваш взгляд, дополнительного хранителя экрана winexit.scr перед стандартными хранителями экрана?
- какие угрозы безопасности и каналы утечки конфиденциальной информации может устранить программа syskey?
- какая из рассмотренных в данной лабораторной работе программ управления разрешениями на доступ к объектам имеет небезопасную функцию и как могут быть нейтрализованы последствия ее несанкционированного применения?

9. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

- титульный лист с названиями университета (*Московский государственный социальный университет*), факультета (*информатики и информационных технологий*), кафедры (*информационной безопасности*), учебной дисциплины и лабораторной работы, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;
- содержание отчета с постраничной разметкой;
- ответы на вопросы, данные в ходе подготовки к выполнению работы;
- сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы;
- ответы на контрольные вопросы.

Порядок защиты лабораторной работы:

1. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы, содержание которого соответствует п. 9 порядка выполнения работы;

2. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.

3. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.

4. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

Приложение

Стандартные типы доступа к объектам в операционной системе Windows XP

- SINCHRONIZE – использовать объект для синхронизации;
- WRITE_OWNER – изменить владельца объекта;
- WRITE_DAC – изменить дискреционный список контроля доступа к объекту;
- READ_CONTROL – прочитать данные из дискреционного списка контроля доступа;
- DELETE – удалить объект.

Специальные права доступа к объектам

- READ_DATA – прочитать данные из объекта;
- WRITE_DATA – записать данные в объект;
- APPEND_DATA – добавить данные в объект;
- READ_ATTRIBUTES – прочитать атрибуты объекта;
- WRITE_ATTRIBUTES – записать атрибуты объекта;
- READ_EA – прочитать расширенные атрибуты объекта;
- WRITE_EA – записать расширенные атрибуты объекта;
- EXECUTE – выполнить программный файл.

Родовые права доступа к объектам

- GENERIC_READ - READ_CONTROL, READ_DATA, READ_ATTRIBUTES, READ_EA, SINCHRONIZE;

- GENERIC_WRITE - READ_CONTROL, WRITE_DATA, WRITE_ATTRIBUTES, WRITE_EA, APPEND_DATA, SINCHRONIZE;
- GENERIC_EXECUTE - READ_CONTROL, READ_ATTRIBUTES, EXECUTE, SINCHRONIZE.

Список использованных источников

1. Малюк, А.А. Введение в информационную безопасность. Учебное пособие для вузов [Текст] / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. – М.: Горячая линия-Телеком, 2014. – 290 с.: ил. (библиотека ГГНТУ)

2. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высших учебных заведений [Текст] / В.П. Мельников, С.А. Клейменов, А.М, Петраков; под ред. С.А. Клейменова - М.: Издательский центр «Академия», 2008. – 336 с. (библиотека ГГНТУ)

3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие [Текст] / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.: ил. (библиотека ГГНТУ)

4. Грибунин, В.Г. Комплексная система защиты информации на предприятии. Учебное пособие [Текст] / В.Г. Грибунин, В.В. Чудовский - М.: Издательский центр «Академия», 2009. - 416 с. (библиотека ГГНТУ)

5. Стрельцов, А.А. Организационно-правовое обеспечение информационной безопасности. Учебное пособие для вузов [Текст] / А.А. Стрельцов, В.С. Горбатов, Т.А.Полякова, Т.А. Кондратьева, О. В. Дамаскин, Е. Б. Белов, С. Ю. Савин - М.: Академия, 2008. - 256 с. (библиотека ГГНТУ)