**Кафедра цифровой экономики**

## Лабораторный практикум по дисциплине

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Методические указания**
**к лабораторным работам для студентов**
**направлений подготовки:**
**38.03.05 «Бизнес-информатика» (степень - бакалавр)**
**специальности:**

Ульяновск

2017

**Лабораторная работа №1**

**Идентификация и аутентификация пользователей в защищенных версиях операционной системы Windows**

Цель работы: освоение средств администратора защищенных версий операционной системы Windows, предназначенных для

- регистрации пользователей и групп в системе,
- определения их привилегий,
- определения параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе.

Подготовка к выполнению работы: подготовить для включения в отчет о лабораторной работе определения понятий

- *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. После собеседования с преподавателем и получения допуска к работе войти в систему под указанным именем (с правами администратора).
2. 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, введя в качестве строки описания текст «Студент группы БИ-О-2011»);
- включить в отчет о лабораторной работе
  - ♦ копию экранной формы создания новой учетной записи,
  - ♦ копию экранной формы со списком зарегистрированных пользователей,
  - ♦ список команд контекстного меню (при отсутствии выделения имени пользователя в списке),
  - ♦ 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
  - ♦ когда должна применяться команда «Задать пароль»,
  - ♦ в чем опасность ее применения,
  - ♦ как должна происходить смена пароля пользователем.

3. 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.

4. 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.

5. 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.

6. Включить в отчет по лабораторной работе ответы на контрольные вопросы:

- каковы основные цели угроз безопасности информации в компьютерных системах?
- насколько средства, изученные при выполнении лабораторной работы, могут нейтрализовать эти угрозы?
- каковы другие признаки, в соответствии с которыми может быть проведена классификация угроз безопасности в компьютерных системах?
- каковы основные каналы утечки конфиденциальной информации в компьютерных системах?
- насколько средства, изученные при выполнении лабораторной работы, могут перекрыть эти каналы?

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

- титульный лист с названиями университета (*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ульяновский государственный университет*), факультета (*финансов и учета*), кафедры (цифровой экономики), учебной дисциплины и лабораторной работы, номером варианта, 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. 7 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 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 1

| **Номер варианта** | **Поясняемые привилегии пользователей** |
|---|---|
| 1 | Доступ к компьютеру из сети<br>Работа в режиме операционной системы<br>Добавление рабочих станций в домен<br>Настройка квот памяти для процесса<br>Управление аудитом и журналом безопасности |
| 2 | Локальный вход в систему<br>Разрешать вход в систему через службу терминалов<br>Архивирование файлов и каталогов<br>Обход перекрестной проверки<br>Изменение параметров среды оборудования |
| 3 | Отказ в доступе к компьютеру из сети<br>Изменение системного времени<br>Создание файла подкачки<br>Создание маркерного объекта<br>Выполнение задач по обслуживанию томов |
| 4 | Завершение работы системы<br>Создание постоянных объектов совместного использования<br>Отладка программ<br>Отклонить локальный вход<br>Профилирование одного процесса |
| 5 | Отключение компьютера от стыковочного узла<br>Запретить вход в систему через службу терминалов<br>Разрешение доверия к учетным записям компьютеров и пользователей при делегировании<br>Принудительное удаленное завершение работы<br>Отказ во входе в качестве пакетного задания |
| 6 | Доступ к компьютеру из сети<br>Создание журналов безопасности<br>Увеличение приоритета диспетчирования |

| | |
|---|---|
| | Загрузка и выгрузка драйверов устройств<br>Профилирование загруженности системы |
| 7 | Локальный вход в систему<br>Закрепление страниц в памяти<br>Вход в качестве пакетного задания<br>Вход в качестве службы<br>Замена маркера уровня процесса |
| 8 | Отказ в доступе к компьютеру из сети<br>Восстановление файлов и каталогов<br>Синхронизация данных службы каталогов<br>Смена владельца файлов или иных объектов<br>Отказ во входе в качестве службы |

## Лабораторная работа №2

## Реализация политики безопасности в защищенных версиях операционной системы Windows

Цель работы: освоения средств администратора и аудитора защищенных версий операционной системы Windows, предназначенных для

- определения параметров политики безопасности;
- определения параметров политики аудита;
- просмотра и очистки журнала аудита.

Подготовка к выполнению работы: по материалам изученных ранее дисциплин или учебных пособий вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

- *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. После собеседования с преподавателем и получения допуска к работе войти в систему под указанным именем (с правами администратора).

2. 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.

3. 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 | 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.

4. 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.

5. 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.

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

- в чем уязвимость с точки зрения безопасности информации принимаемая по умолчанию реакция системы на превышение размера журнала аудита?
- какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
- из каких этапов состоит построение политики безопасности для компьютерной системы?
- к чему может привести ошибочное определение политики безопасности (приведите примеры)?
- почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

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

- титульный лист с названиями университета (*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ульяновский государственный университет*), факультета (*финансов и учета*), кафедры (цифровой экономики), учебной дисциплины и лабораторной работы, номером варианта, 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:

5. 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. 7 порядка выполнения работы;
6. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
7. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
8. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

Приложение 1

| **Номер варианта** | **Поясняемые параметры политики безопасности** |
|---|---|
| 1 | Учетные записи: состояние учетной записи «Администратор» Устройства: разрешено форматировать и извлекать съемные носители<br>Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию<br>Клиент сети Microsoft: использовать цифровую подпись (всегда)<br>Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля |
| 2 | Учетные записи: состояние учетной записи «Гость»<br>Устройства: разрешать отстыковку без входа в систему<br>Контроллер домена: запретить изменение пароля учетных записей компьютера<br>Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)<br>Сетевая безопасность: принудительный вывод из сеанса по истечении допустимых часов работы |
| 3 | Учетные записи: ограничить использование пустых паролей только для консольного входа<br>Устройства: запретить пользователям установку драйверов принтера<br>Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала<br>Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам<br>Сетевая безопасность: уровень проверки подлинности LAN Manager |
| 4 | Учетные записи: переименование учетной записи администратора<br>Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям<br>Член домена: шифрование данных безопасного канала, когда это возможно<br>Сервер сети Microsoft: длительность простоя перед отключением сеанса<br>Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC) |
| 5 | Учетные записи: переименование учетной записи гостя |

| | |
| --- | --- |
| | Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям<br>Член домена: цифровая подпись данных безопасного канала, когда это возможно<br>Сервер сети Microsoft: использовать цифровую подпись (всегда)<br>Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC) |
| 6 | Завершение работы: разрешить завершение работы системы без выполнения входа в систему<br>Устройства: поведение при установке неподписанного драйвера<br>Член домена: максимальный срок действия пароля учетных записей компьютера<br>Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)<br>Доступ к сети: разрешить трансляцию анонимного SID в имя |

| Номер варианта | Поясняемые параметры политики безопасности |
|---|---|
| 7 | Завершение работы: очистка страничного файла виртуальной памяти<br>Член домена: требует стойкого ключа сеанса (Windows 2000 или выше)<br>Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями<br>Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования<br>Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей |
| 8 | Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов<br>Член домена: отключить изменение пароля учетных записей компьютера<br>Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями<br>Консоль восстановления: разрешить автоматический вход администратора<br>Сетевой доступ: разрешать анонимный доступ к общим ресурсам |
| 9 | Системные объекты: учитывать регистр для подсистем, отличных от Windows<br>Сетевой доступ: не разрешать средству сохранения имен пользователей и паролей сохранять пароли или учетные данные для проверки в домене<br>Сетевой доступ: пути в реестре доступны через удаленное подключение<br>Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам<br>Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа |
| 10 | Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)<br>Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям<br>Сетевой доступ: разрешать анонимный доступ к именованным каналам |

| | |
|---|---|
| | Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)<br>Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки |

## Лабораторная работа №3

## Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Цель работы: освоение средств защищенных версий операционной системы Windows, предназначенных для

- разграничения доступа субъектов к папкам и файлам;
- разграничения доступа субъектов к принтерам;
- разграничения доступа к разделам реестра;
- обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

Подготовка к выполнению работы: по материалам изученных ранее дисциплин или учебных пособий вспомнить и 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:

7. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами обычного пользователя).
8. Освоить средства разграничения доступа пользователей к папкам:

- выполнить команду «Общий доступ и безопасность» контекстного меню папки, содержащей отчеты студентов 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.

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

- какая политика безопасности лежит в основе разграничения доступа к объектам в защищенных версиях операционной системы Windows?
- в чем уязвимость принятой в защищенных версиях операционной системы Windows политики разграничения доступа (приведите примеры)?
- как работает механизм наследования при определении прав на доступ субъектов к объектам в защищенных версиях операционной системы Windows?
- какие дополнительные возможности разграничения доступа к информационным ресурсам предоставляет шифрующая файловая система?
- насколько, на Ваш взгляд, удобно использование шифрующей файловой системы (в том числе при необходимости совместной работы над документами)?
- какой стандартный механизм работы с личными и общими документами предлагается в защищенных версиях операционной системы Windows и насколько, на Ваш взгляд, он удобен?

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

- титульный лист с названиями университета (*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ульяновский государственный университет*), факультета (*финансов и учета*), кафедры (цифровой экономики), учебной дисциплины и лабораторной работы, номером варианта, 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:

9. 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;
10. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
11. По результатам защиты каждому студенту выставляется дифференцированная

оценка, учитываемая в при определении его итогового рейтинга за семестр.

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

## Лабораторная работа № 4

## Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов

Цель работы: освоение средств программной системы PGP, предназначенных для

- шифрования конфиденциальных ресурсов для разграничения доступа к ним;
- обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи;
- надежного уничтожения остаточной конфиденциальной информации;
- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

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», «Криптографические методы и средства обеспечения информационной безопасности» и другим) вспомнить и подготовить для включения в отчет о лабораторной работе определения понятий

- *алгоритмы симметрического шифрования*;
- *алгоритмы асимметрического шифрования*;
- *электронная цифровая подпись*;
- *безопасные генерация, хранение и распространение ключей симметрического шифрования;*
- *сертификат открытого ключа асимметрического шифрования*;
- *функции хеширования*.

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

14) каковы основные параметры симметрических криптографических систем?
15) какие виды современных симметрических криптосистем Вы знаете?
16) какие асимметрические криптосистемы Вам известны, чем они отличаются друг от друга?
17) каковы основные этапы алгоритмов получения и проверки электронной цифровой подписи?
18) какие требования предъявляются к идеальному (абсолютно стойкому по К.Шеннону) алгоритму симметрического шифрования?
19) как должен создаваться, храниться и распространяться ключ симметрического шифрования?

20) какая информация содержится в сертификате открытого ключа асимметрического шифрования?

21) какие требования предъявляются к функциям хеширования?

22) какие функции хеширования Вам известны и чем они различаются?

Порядок выполнения работы:

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

10. Установить программную систему PGP 6.0.2, запустив программу Setup.exe из папки C:\Disrtrib\PGP\6.0.2. Выбрать для установки только следующие компоненты:

- PGP 6.0.2 Program Files;
- PGP 6.0.2 User’s Manual;
- Unconfigured PGP 6.0.2 Client Install;
- PGPdisk for Windows.

На вопрос программы установки о существовании ключей ответить «Нет», а на вопрос о необходимости перезагрузки системы - «Да».

11. Запустить программу PGPtools (с помощью меню «Пуск» или значка PGPtray на панели задач), ознакомиться и отразить в отчете о лабораторной работе состав программных средств, входящих в систему PGP (при необходимости воспользоваться справкой о системе PGP).

12. Создать криптографические ключи с помощью программы PGPkeys. Включить в отчет о лабораторной работе сведения о порядке создания ключей шифрования в системе PGP и копии используемых при этом экранных форм, а также ответы на вопросы:

- как обеспечивается случайность выбираемых криптографических ключей в системе PGP;
- как и где хранится секретный ключ пользователя в системе PGP;
- как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной потере.

13. Изучить (на примере документов с отчетами о ранее выполненных Вами лабораторных работах, обычных текстовых файлов, файлов изображений только из своей папки) способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы PGPtools. При необходимости отменить защиту файлов собственной папки с помощью шифрующей файловой системы Windows. Включить в отчет о данной лабораторной работе сведения о порядке шифрования и расшифрования файлов в системе PGP, копии используемых при этом экранных форм и ответы на вопросы:

- какие дополнительные параметры шифрования могут быть использованы и в чем их смысл и возможное применение (обязательно проверить на примере и результаты проверки отразить в отчете);

- как генерируется, как и где хранится ключ симметрического шифрования файла в системе PGP;
- как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей;
- изменяется ли и как размер файла после его шифрования.

6. Изучить (на примере документов из своей папки) способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы PGPtools. Включить в отчет сведения о порядке обеспечения аутентичности и целостности электронных документов в системе PGP, копии используемых при этом экранных форм и ответы на вопросы:

- какие дополнительные параметры получения электронной цифровой подписи могут быть использованы, в чем их смысл и возможное применение (обязательно проверить на примере и результаты проверки отразить в отчете);
- какова реакция на программы на нарушение целостности подписанного документа (обязательно проверить на примере и результаты проверки отразить в отчете).

7. Изучить способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в системе PGP с помощью функций Encrypt Sign и Decrypt/Verify программы PGPtools. Включить в отчет сведения о порядке одновременного обеспечения конфиденциальности, аутентичности и целостности электронных документов в этой системе, а также копии используемых при этом экранных форм.
8. Изучить способы надежного удаления файлов с конфиденциальной информацией с помощью функции Wipe программы PGPtools. Включить в отчет сведения о порядке уничтожения конфиденциальных электронных документов в системе PGP и копии используемых при этом экранных форм.
9. Изучить способы надежного уничтожения остаточной информации, которая может содержать конфиденциальные сведения, с помощью функции Freespace Wipe программы PGPtools. Включить в отчет сведения о назначении и порядке использования этой программы, копии используемых в ней экранных форм и ответы на вопросы:

- как достигается надежное уничтожение остаточной конфиденциальной информации в системе PGP;
- является ли подобный метод уничтожения абсолютно надежным и, если нет, как может быть обеспечено абсолютно надежное уничтожение остаточной информации

10. Изучить способы создания электронного хранилища конфиденциальных документов с помощью программы PGPdisk. Создать (с помощью функции New программы PGPdisk) новый PGP диск на локальном диске c: (в папке Учебные материалы \ КЗИ2000) размером 1 Mb и защитить его с помощью парольной фразы. Выполнить быстрое форматирование созданного диска (указав файловую систему FAT). Скопировать в созданный PGP диск папку с собственными документами. Размонтировать созданный диск с помощью функции Unmount программы PGPdisk и завершить работу с этой

программой. Завершить сеанс работы с Windows и снова войти в систему под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1. Попытаться получить доступ к файлам, размещенным в виртуальном диске. Завершить сеанс работы с Windows и возобновить его под именем обобщенной учетной записи. Смонтировать (с помощью функции Mount программы PGPdisk) созданный PGP диск, удалить из него все файлы, размонтировать и уничтожить его (с помощью функции Wipe программы PGP). Включить в отчет сведения о назначении и порядке использования программы PGPdisk, копии используемых экранных форм и ответы на вопросы:

- как защищаются файлы и папки, помещенные в виртуальный PGP диск;
- в чем отличие программы PGPdisk от шифрующей файловой системы операционной системы Windows и в чем общие черты этих систем;
- какая из этих систем, на Ваш взгляд, более удобна для защиты конфиденциальной информации и почему.

11. Изучить способы быстрого выполнения функций системы PGP с помощью программы PGPtray, ярлык которой размещен в правой части панели задач. Включить в отчет сведения о назначении и порядке использования этой программы, а также копии используемых экранных форм.
12. Изучить способы управления настройками системы PGP при ее использовании в организациях с помощью программы PGPadmin (пройти все шаги диалога с мастером вплоть до последнего, на котором вместо кнопки «Save» нажать кнопку «Отмена»). Включить в отчет сведения о возможностях и порядке администрирования системы PGP, копии используемых при этом экранных форм и ответы на вопросы:

- какие функции по управлению шифрованием и обеспечением целостности информационных ресурсов предоставляет администратору программа PGPAdmin;
- какие функции по управлению криптографическими ключами пользователей PGP предоставляет администратору программа PGPadmin;
- какие возможности предоставляет программа PGPadmin по управлению доступными для пользователей функциями программы PGP и где сохраняется подобная информация.

13. Изучить состав программной документации, поставляемой с системой PGP. Включить в отчет сведения о составе программной документации и кратком содержании руководств:

- пользователя PGP;
- администратора PGP;
- по установке PGP.

14. После проверки отчета преподавателем удалить систему PGP, установленную при выполнении п. 2, с помощью функции «Установка и удаление программ» *Панели управления* Windows.
15. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

- как выбрать длину криптографического ключа в системе PGP?
- в чем разница между контролем неизменности объекта и контролем его целостности?
- какие объекты и субъекты участвуют в процессе контроля целостности?
- от чего зависит надежность алгоритма контроля целостности?
- почему в процессе контроля целостности объекта важно обеспечить контроль реальных данных?
- в чем заключается достаточное условие чтения реальных данных?
- насколько, на Ваш взгляд надежные методы криптографической защиты используются в программе PGP?
- зачем в составе программы PGP предусмотрены административные функции?

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

17. титульный лист с названиями университета (*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ульяновский государственный университет*), факультета (*финансов и учета*), кафедры (цифровой экономики), учебной дисциплины и лабораторной работы, номером варианта, 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:

13. 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;
14. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
15. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
16. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

## 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:

23) что такое Trusted Computer System Evaluation Criteria (TCSEC)?
24) какие основные категории требований к защищенности компьютерных систем предложены в TCSEC, в чем их смысл?
25) какие требования к компьютерным системам предъявляются по классу защиты C2 TCSEC?
26) кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?
27) как должны использоваться записи журнала аудита событий безопасности?
28) какие права доступа к файлу аудита имеет по умолчанию администратор системы?
29) что такое консольное приложение Windows?

Порядок выполнения работы:

14. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами администратора).
15. 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.

16. 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 с;

- 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.

17. 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.

18. 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.

7. 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.

9. 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:

10. титульный лист с названиями университета (*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ульяновский государственный университет*), факультета (*финансов и учета*), кафедры (цифровой экономики), учебной дисциплины и лабораторной работы, номером варианта, 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.

<u>Порядок защиты лабораторной работы</u>:

17. 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;

18. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
19. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.
20. 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.

## Лабораторная работа № 6

## Изучение штатных средств операционной системы Windows XP, предназначенных для обеспечения информационной безопасности при использовании глобальных вычислительных сетей

Цель работы: освоение системных средств Windows XP, предназначенных для

- настройки ограничений, регулирующих обмен данными между Интернетом и домашней или небольшой офисной сетью;
- настройки зон безопасности узлов Интернета при использовании браузера (обозревателя) Internet Explorer;
- настройки уровней конфиденциальности Internet Explorer при доступе к узлам различных зон Интернета;
- настройки правил автоматической обработки сообщений электронной почты при использовании программы Outlook Express;
- ограничения доступа к отдельным узлам Интернета при использовании Internet Explorer.

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

- *протокол (применительно к вычислительным сетям)*;
- *модель OSI*;
- *порт (применительно к сетевым программам)*;
- *межсетевой экран (брандмауэр, firewall)*;
- *правила разграничения доступа*;
- *спам*.

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

30) какие подходы к анализу и оценке защищенности распределенных вычислительных систем (РВС) Вы знаете и какой из них следует использовать для сетей предприятий с использованием Интернет (и почему)?
31) в чем заключаются типовые угрозы безопасности РВС и каковы их цели?
32) что такое TCP/IP?
33) в чем основная причина уязвимости компьютеров, подключенных к сети Интернет?
34) в чем состоят требования к безопасному каналу связи?
35) какие основные функции должны быть синтезированы в системе комплексной защиты

информации в РВС в соответствии с документом Trusted Network Interpretation?

Порядок выполнения работы:

19. После собеседования с преподавателем и получения допуска к работе войти в систему с обобщенным именем учетной записи (с правами администратора).
20. Освоить работу с входящим в состав Windows XP программным средством Internet Connection Firewall (ICF):

- ознакомиться с разделом Справки Windows «Общие сведения о брандмауэре подключения к Интернету» и включить в отчет о лабораторной работе краткие сведения о назначении и функционировании ICF и его журнале безопасности;
- открыть окно включения и настройки ICF (Пуск | Панель управления | Сетевые подключения | Подключение по локальной сети | Свойства | Дополнительно);
- включить выключатель «Защитить мое подключение к Ин6тернету» и нажать кнопку «Параметры»;
- пользуясь информацией с вкладки «Службы», включить в отчет о лабораторной работе сведения о запущенных на защищаемом компьютере сетевых службах, к которым может быть разрешен доступ из Интернета, и их назначении, а также ответ на вопрос, в чем опасность подобного разрешения;
- нажать кнопку «Добавить» и включить в отчет о лабораторной работе сведения о порядке добавления новых сетевых служб, которые установлены на защищаемом компьютере и к которым разрешен доступ из Интернета, после чего нажать кнопку «Отмена»;
- нажать кнопку «Изменить» и включить в отчет о лабораторной работе сведения о порядке изменения параметров установленных на защищаемом компьютере сетевых служб, после чего нажать кнопку «Отмена»;
- открыть вкладку «Ведение журнала безопасности» и включить в отчет о лабораторной работе сведения о параметрах ведения и параметрах файла журнала безопасности ICF, а также ответы на вопросы, ведется ли по умолчанию журнал безопасности ICF и что происходит при его переполнении;
- открыть вкладку ICMP и включить в отчет о лабораторной работе сведения о входящих на защищаемый компьютер управляющих пакетах (запросах), для которых может быть разрешена отправка ответных пакетов, и их назначении;
- нажать кнопку «Отмена» (вернуться в окно свойств подключения по локальной сети) и еще раз нажать кнопку «Отмена»;
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта.

21. Освоить средства управления уровнями безопасности узлов Интернета при использовании Internet Explorer:

- ознакомиться с разделом «Использование обозревателя Internet Explorer» Справки

Windows и с разделами «Общие сведения об обеспечении безопасности и конфиденциальности», «Защита компьютера от небезопасных программ» и «Общие сведения о зонах безопасности» Internet Explorer и включить в отчет о лабораторной работе сведения о назначении средств безопасности браузера (обозревателя) Internet Explorer;

- открыть окно настройки средств безопасности Internet Explorer (Пуск | Панель управления | Свойства обозревателя | Безопасность);
- выбрать зону ограниченных узлов и нажать кнопку «Узлы»;
- включить в отчет о лабораторной работе сведения о порядке добавления и удаления узлов из той или иной зоны, после чего нажать кнопку «Отмена»;
- включить в отчет о лабораторной работе описание выбранной зоны безопасности и рекомендуемого для нее уровня безопасности;
- нажать кнопку «Другой» и включить в отчет о лабораторной работе сведения о параметрах безопасности, установленных по умолчанию для выбранной зоны, после чего нажать кнопку «Отмена»;
- повторить выполнение трех предыдущих пунктов для остальных зон безопасности, после чего нажать кнопку «Отмена»;
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и ответ на вопрос, как изменить назначенный по умолчанию уровень безопасности для той или иной зоны узлов Интернета.

22. Освоить средства настройки уровней конфиденциальности при доступе к узлам Интернета с помощью Internet Explorer:

- ознакомиться с разделами «Общие сведения об обеспечении безопасности и конфиденциальности», «Общие сведения о политике конфиденциальности» и «Общие сведения о файлах “cookie”» Справки Internet Explorer;
- включить в отчет о лабораторной работе краткие сведения о возможностях утечки конфиденциальных данных при доступе к отдельным узлам Интернета и о способах обеспечения конфиденциальности в Internet Explorer;
- открыть окно настройки средств конфиденциальности Internet Explorer (Пуск | Панель управления | Свойства обозревателя | Конфиденциальность);
- переместить «ползунок» в крайнее нижнее положение («Принимать все “cookie”») и включить в отчет о лабораторной работе характеристику данной зоны конфиденциальности;
- нажать кнопку «Дополнительно», ознакомиться с составом и порядком назначения дополнительных параметров конфиденциальности, перекрывающих установленную по умолчанию для выбранной зоны автоматическую обработку, и включить данные сведения в отчет о лабораторной работе, после чего нажать кнопку «Отмена»;
- переместить «ползунок» на одно положение вверх и включить в отчет о лабораторной работе характеристику данной зоны конфиденциальности;

- нажать кнопку «Изменить» и включить в отчет о лабораторной работе сведения о порядке изменения параметров конфиденциальности для отдельных узлов Интернета, после чего закрыть окно изменения параметров;
- перемещая «ползунок» вверх, ознакомиться и включить в отчет о лабораторной работе характеристики оставшихся зон конфиденциальности, после чего нажать кнопку «Отмена»;
- открыть окно для просмотра и удаления файлов “cookie” (Пуск | Панель управления | Свойства обозревателя | Общие), нажать последовательно кнопки «Параметры» и «Просмотр файлов», включить в отчет о лабораторной работе сведения о порядке просмотра файлов “cookie”, после чего нажать кнопку «Отмена»;
- включить в отчет о лабораторной работе ответы на вопросы, в какой папке сохраняются файлы “cookie” и какие разрешения на доступ к этой папке установлены по умолчанию;
- нажать кнопку «Удалить “cookie”», включить в отчет о лабораторной работе сведения о порядке удаления файлов “cookie”, после чего дважды нажать кнопку «Отмена»;
- ознакомиться с разделом «Безопасное предоставление доступа к личным сведениям» Справки Internet Explorer и включить в отчет о лабораторной работе сведения о назначении и защите профиля с личными данными пользователя;
- открыть окно настройки профиля с личными данными пользователя Internet Explorer (Пуск | Панель управления | Свойства обозревателя | Содержание) и нажать кнопку «Профиль»;
- ознакомиться с порядком создания и содержанием профиля пользователя, включить в отчет о лабораторной работе данные сведения, нажать кнопку «отмена» для закрытия окна настройки свойств обозревателя;
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта.

23. Освоить средства настройки правил для автоматической обработки сообщений электронной почты при использовании программы Outlook Express:

- начать работу с программой Outlook Express (с помощью меню «Пуск»);
- открыть окно создания правил для входящей почты (Сервис | Правила для сообщений | Почта | Создать);
- используя информацию из раздела «Как создать правило для почтовых сообщений?» Справки Outlook Express, освоить создание правил автоматической обработки входящих сообщений (определение условия отбора сообщений и автоматически совершаемых над этими сообщениями действий);
- применить полученные навыки для создания правила, препятствующего загрузке на компьютер пользователя незапрашиваемых рекламных сообщений (спама);
- включить в отчет о лабораторной работе сведения о порядке создания и изменения правил для автоматической обработки почты в Outlook Express;

- открыть окно создания правил для блокирования сообщений от определенных отправителей (Сервис | Правила для сообщений | Почта | Список блокируемых отправителей);
- используя информацию из раздела «Как блокировать сообщения от определенного отправителя или домена?» Справки Outlook Express, освоить создание правил блокирования входящих сообщений и включить соответствующие сведения в отчет о лабораторной работе;
- включить в отчет о лабораторной работе ответы на вопросы, что происходит с сообщениями от блокируемых отправителей и в чем ограничение применения данного подхода;
- завершить работу с программой Outlook Express и включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта.

8. Освоить средства ограничения доступа к отдельным узлам Интернета при использовании Internet Explorer:

- открыть окно ограничения доступа к информации, получаемой из Интернета (Пуск | Панель управления | Свойства обозревателя | Содержание | Общие);
- используя информацию из Справки Internet Explorer (раздел «Использование ограничения доступа»), включить в отчет сведения о назначении, порядке создания и использования пароля-допуска, ограничивающего доступ к определенным узлам Интернета;
- открыть вкладку «Разрешенные узлы» в том же окне и включить в отчет о лабораторной работе сведения о порядке запрещения доступа к узлам глобальной сети независимо от оценок их содержания;
- закрыть окно свойств обозревателя и включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта.

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

- что такое удаленное сканирование портов и для чего оно может проводиться?
- в чем сущность методов открытого и анонимного сканирования портов?;
- в чем основные причины успеха удаленных атак на РВС?;
- какие существуют основные методы защиты РВС?
- в чем основные функции, достоинства и недостатки межсетевых экранов?
- к какому классу защищенности (в соответствии с руководящими документами Гостехкомиссии РФ) может быть отнесен встроенный в Windows XP брандмауэр подключения к Интернету?
- какие основные параметры доступа к узлам Интернета изменяются для различных его зон (в терминологии Internet Explorer) и почему именно эти параметры?
- в чем недостатки рассмотренных в настоящей работе методов защиты от спама?

8. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:
9. титульный лист с названиями университета (*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ульяновский государственный университет*), факультета (*финансов и учета*), кафедры (цифровой экономики), учебной дисциплины и лабораторной работы, номером варианта, 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:

21. 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. 8 порядка выполнения работы;
22. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.
23. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая при определении его итогового рейтинга за семестр.
24. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.