ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВА

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕГОРОДА МОСКВЫ

«КОЛЛЕДЖ СВЯЗИ №54»

ИМЕНИ П.М.ВОСТРУХИНА

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

для **МДК 03.02. Программно-аппаратные средства защиты информации**

специальность 090905 Организация и технология защиты информации

Москва 2015.

|  |  |
| --- | --- |
| РАССМОТРЕНЫПредметной цикловой комиссиейПротокол № \_\_\_1\_\_Председатель ПЦК\_\_\_\_\_\_\_\_\_\_\_« 31 » августа 2015г. | УТВЕРЖДАЮЗам. директора по УМРГБПОУ КС № 54\_\_\_\_\_\_\_\_\_\_И.Г. Бозрова«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2015 г. |

Разработчик:

Бастрыкин К.М., преподаватель ГБПОУ КС №54

**Содержание**

1. Общие положения.

2. Методика и средства выполнения практических работ

3. Этапы выполнения практических работ

4.Правила выполнения практических работ

5.Критерии оценки практических работ

6.Правила внутреннего распорядка и техника безопасности при выполнении практических работ

7. Тематика практических работ и задания к ним

8. Учебно-методическое и информационное обеспечение МДК

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

Методические указания для выполнения практических работ по МДК 03.02. Программно-аппаратные средства защиты информации составлены в соответствии с рабочей программой ПМ.01 Организация работ подразделений защиты информации.

Профессиональный модуль ПМ.01 Организация работ подразделений защиты информации взаимосвязан с учебными дисциплинами специальности 090905 Организация и технология защиты информации ОП.01 Основы теории информации, ОП.02 Технологии физического уровня передачи данных, ОП.03 Архитектура аппаратных средств, ОП.04 Операционные системы, ОП.05 Основы программирования и баз данных.

Целью выполнения практических работ является овладение указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями. В ходе освоения профессионального модуля обучающийсядолжен:

**иметь практический опыт:**

* уча­стия в тех­ни­че­ской экс­плуа­та­ции за­щи­щен­ных объ­ек­тов про­фес­сио­наль­ной дея­тель­но­сти;
* при­ме­не­ния тех­ни­че­ских средств за­щи­ты ин­фор­ма­ции;
* вы­яв­ле­ния воз­мож­ных уг­роз ин­фор­ма­ци­он­ной безо­пас­но­сти при ра­бо­те за­щи­щен­ных объ­ек­тов про­фес­сио­наль­ной дея­тель­но­сти.

 **уметь:**

* ра­бо­тать с тех­ни­че­ски­ми сред­ст­ва­ми за­щи­ты ин­фор­ма­ции;
* ра­бо­тать с за­щи­щен­ны­ми ав­то­ма­ти­зи­ро­ван­ны­ми сис­те­ма­ми;
* пе­ре­да­вать ин­фор­ма­цию по за­щи­щен­ным ка­на­лам свя­зи;
* фик­си­ро­вать от­ка­зы в ра­бо­те средств вы­чис­ли­тель­ной тех­ни­ки.

**знать:**

* ви­ды, ис­точ­ни­ки и но­си­те­ли за­щи­щае­мой ин­фор­ма­ции;
* ис­точ­ни­ки опас­ных сиг­на­лов;
* струк­ту­ру, клас­си­фи­ка­цию и ос­нов­ные ха­рак­те­ри­сти­ки тех­ни­че­ских ка­на­лов утеч­ки
ин­фор­ма­ции;
* клас­си­фи­ка­цию тех­ни­че­ских раз­ведок и методы про­ти­во­дей­ст­вия им;
* ме­то­ды и средства ин­же­нер­но-тех­ни­че­ской за­щи­ты ин­фор­ма­ции;
* ме­то­ды скры­тия ин­фор­ма­ции;
* про­грамм­но-ап­па­рат­ные сред­ст­ва за­щи­ты информации;
* струк­ту­ру под­сис­те­мы безо­пас­но­сти опе­ра­ци­он­ных сис­тем и вы­пол­няе­мые ею функ­ции;
* сред­ст­ва за­щи­ты в вы­чис­ли­тель­ных се­тях;
* сред­ст­ва обес­пе­че­ния за­щи­ты ин­фор­ма­ции в системах управления базами данных;
* кри­те­рии за­щи­щен­но­сти компьютерных систем;
* ме­то­ди­ки про­вер­ки за­щи­щен­но­сти объ­ек­тов ин­фор­ма­ти­за­ции на со­от­вет­ст­вие тре­бо­ва­ни­ям нор­ма­тив­ных до­ку­мен­тов.

**Выполнение практическихработспособствуютформированию:**

Профессиональных и общих компетенций:

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 3.1. | При­ме­нять про­грамм­но-ап­па­рат­ные и ин­же­нер­но-тех­ни­че­ские сред­ст­ва за­щи­ты ин­фор­ма­ции на объ­ек­тах про­фес­сио­наль­ной дея­тель­но­сти. |
| ПК 3.2. | Уча­ст­во­вать в экс­плуа­та­ции за­щи­щен­ных объ­ек­тов |
| ПК 3.3. | Про­во­дить рег­ла­мент­ные ра­бо­ты и фик­си­ро­вать от­ка­зы средств за­щи­ты |
| ПК 3.4. | Вы­яв­лять и ана­ли­зи­ро­вать воз­мож­ные уг­ро­зы ин­фор­ма­ци­он­ной безо­пас­но­сти объ­ек­тов |
| ОК 1. | Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. |
| ОК 2. | Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество |
| ОК 3. | Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях. |
| ОК 4. | Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития. |
| ОК 5. | Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности. |
| ОК 6. | Работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7. | Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий. |
| ОК 8. | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9. | Быть готовым к смене технологий в профессиональной деятельности. |
| ОК 10. | Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). |
| ОК 11. | Применять математический аппарат для решения профессиональных задач. |
| ОК 12. | Оценивать значимость документов, применяемых в профессиональной деятельности. |
| ОК 13. | Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность. |

В результате выполнения практических работ обучающиеся получат практический опыт обеспечения информационной безопасности функционирования систем, научатся эксплуатировать средства информационной безопасности БД.

**МЕТОДИКА И СРЕДСТВА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ**

Выбор содержания и объем конкретной практической работы обусловлен сложностью учебного материала для усвоения, междисциплинарными связями и учетом значения конкретной практической работы для приобретения обучающимися соответствующих умений и компетенций, предусмотренных ФГОС.

Методика выполнения каждой практической работы определяется моделью соответствующей задачи, решаемой студентом на занятии по заданию преподавателя.

Средством проведения практических работ являются:

* Комплект персональных ЭВМ в компьютерных классах, с выходом в ГКС Интернет;

Комплекс программного обеспечения:

* операционная система WindowsХР, Vista и др.;

Практические работы проводятся в компьютерных классах, расположенных на учебных площадках.

Процедурным обеспечением практических работ является:

* настоящие Методические указания.
1. **ЭТАПЫ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ**

Выполнение каждой из практических работ включает в себя пять (5) основных этапов.

1. Постановка задачи практической работы

На первом практическом занятии со студентами проводится общая постановка задач практических работ. Преподаватель может давать необходимые пояснения по методике предстоящих практических работ. После ознакомления с программным комплексом преподаватель проводит постановку задачи конкретного практического занятия. Здесь разъясняется группе студентов содержание и объем работ, предусмотренных конкретной практической работой. Прежде всего, формулируются цели, задачи, основные этапы работы, последовательность и ход решения задачи практической работы. Определяются содержание и форма представления результатов работы. Необходимо пояснить, что каждая практическая работа студента должна быть оформлена в виде отчета о практической работе. Поясняется методика составления и оформления отчета по практической работе. Проводится инструктаж по Охране труда с записью в журнал.

2. Ознакомление студента с содержанием и объемом практической работы.

На этом этапе студент должен тщательно изучить содержание и объем предстоящей практической работы. Если постановка задачи недостаточно ясна, он может обратиться к преподавателю за дополнительными разъяснениями. Затем студент приступает к выполнению задания практической работы.

1. Порядок выполнения практической работы.

Студент включает ПК и, при необходимости, запускает соответствующую программу. В соответствии с установленной последовательностью этапов работы студент выполняет объем работ, предусмотренных заданием практической работы.

При условии выполнения полного объема практической работы студент проверяет правильность результатов и предъявляет преподавателю результаты работы, выведенные на монитор. В случае замеченных ошибок, студент принимает меры к их исправлению и затем снова предъявляет результаты преподавателю для контроля и приема результатов работы. Если в работе ошибок не содержится, то приступает к составлению и оформлению отчета по практической работе.

1. Регистрация результатов и оформление отчета по практической работе.

По мере того, как выполняются этапы практическойработы, студент регистрирует все результаты своей работы в собственном файле. Этот файл в будущем должен быть оформлен как отчет студента по практической работе. Файл должен храниться в папке соответствующего студента. На основе полученных результатов практической работы, составить соответствующий отчет и сдать его преподавателю. Оформление отчета выполнить по следующим правилам. Отчет по практической работе должен содержать следующие обязательные разделы – номер и тема ПР, цель, задание, основные этапы практической работы, выводы по выполненной работе.

Отчет по каждой практической работе составляется по следующей обобщенной структуре:

* Наименование идентифицирующих признаков: «Отчет по практической работе №\_\_\_\_\_ по теме (наименование темы)».
* Студента (указываются фамилия и инициалы, курс, группа).
* Цель работы. Формулируется в соответствии с содержанием раздела «Цель работы», соответствующей практической работы.
* Необходимые принадлежности, задание.

Определяется в соответствии с указанной выше формулировкой и при необходимости уточняется в зависимости от содержания конкретной практической работы.

* Этапы выполнения работы. Последовательно по каждому из этапов приводится характеристика содержания выполненных по этапу работ.
* Выводы по работе. К этой части работы студент должен быть особенно внимательным. Формулируются выводы теоретического и практического характера о выполненной практической работе. Не следует указывать в выводах содержание и объем выполненных работ.

Текст отчета должен быть изложен лаконично и вместе с тем информативно с соблюдением правил грамматики. В конце отчета может быть указана литература, которую студент применил в практической работе. Библиографические описания литературных источников должны быть оформлены в соответствии с ГОСТ 7.1-84. Правила библиографического описания документации.

1. Заключительная часть практической работы.

После окончания составления отчета студент проверяет его правильность и устраняет ошибки. При условии отсутствия ошибок предъявляет экранный отчет преподавателю. Преподаватель читает текст отчета и принимает его. При условии замеченных ошибок преподаватель указывает студенту на эти ошибки. После этого студент исправляет ошибки и повторно предъявляет отчет преподавателю.

После завершения полного объема работ, исправления ошибок по замечаниям преподавателя, сохраняет отчет, выходит из системы и выключает компьютер.

1. **ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ**

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

1. Прежде, чем приступить к выполнению работы, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
2. Перед началом каждой работы проверяется готовность обучающегося к ПР.
3. После выполнения ПР студент должен представить отчет о проделанной работе в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.
4. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
5. Оценка за практическую работу выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

**5. КРИТЕРИИ ОЦЕНКИ ПРАКТИЧЕСКИХ РАБОТ**

Практические работы оцениваются по пятибалльной шкале.

* оценка «5» (отлично) ставится, если работа выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;
* оценка «4» (хорошо) ставится, если работа выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;
* оценка «3» (удовлетворительно) ставится, если работа выполнена в полном объеме, в соответствии с заданием, частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания;
* оценка «2» (неудовлетворительно) ставится, если обучающийся не подготовился к работе, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.
1. **ПРАВИЛА ВНУТРЕННЕГО РАСПОРЯДКА И ТЕХНИКА БЕЗОПАСНОСТИ ПРИ ВЫПОЛНЕНИИ ПРАКТИЧЕСКИХ РАБОТ**

При выполнении практических работ во избежание несчастных случаев, а также преждевременного выхода из строя персональных компьютеров и оборудования студент должен выполнять следующие правила внутреннего распорядка и техники безопасности:

1. К работе в кабинете (лаборатории) допускаются студенты, знакомые с правилами внутреннего распорядка и техники безопасности, изучившие содержание предстоящей практической работы, представившие отчет за предыдущую практическую работу.
2. После ознакомления с правилами внутреннего распорядка и инструктажа по технике безопасности каждый студент должен расписаться в специальном журнале.
3. При работе в кабинете (лаборатории) запрещается приносить собой вещи и предметы, загромождающие рабочие места.
4. Приступая к работе, каждый студент занимает место за «своим» ПК
5. В кабинете (лаборатории) запрещается громко разговаривать, покидать рабочие места без разрешения преподавателя и переходить от одного ПК к другому.
6. Во время небольших перерывов в работе не обязательно выключать компьютер.
7. При появлении запаха гари или при обнаружении повреждения изоляции, обрыва провода следует немедленно сообщить о неисправности преподавателю.
8. Прикасаться к задней панели работающего системного блока (процессора) запрещается.
9. Недопустимо попадание влаги на системный блок, дисплей, клавиатуру и другие устройства.
10. При выполнении практической работы необходимо занять правильную рабочую позу:
* следует сидеть прямо (не сутулясь) и опираться спиной о спинку кресла. Прогибать спину в поясничном отделе нужно не назад, а, наоборот, немного вперед. Недопустимо работать, развалившись в кресле. Такая поза вызывает быстрое утомление, снижение работоспособности.
* Необходимо найти такое положение головы, при котором меньше напрягаются мышцы шеи. Рекомендуемый угол наклона головы – до 20°. В этом случае значительно снижается нагрузка на шейные позвонки и на глаза.
* Положение рук и ног: во время работы за компьютером необходимо расслабить руки, держать предплечья параллельно полу, на подлокотниках кресла, кисти рук – на уровне локтей или немного ниже, запястья – на опорной планке. Тогда пальцы получают наибольшую свободу передвижения. Колени должны располагаться на уровне бедер или немного ниже. При таком положении ног не возникает напряжение мышц. Нельзя скрещивать ноги, класть ногу на ногу – это нарушает циркуляцию крови из-за сдавливания сосудов. Лучше держать обе стопы на подставке или на полу. Необходимо сохранять прямой угол (90°) в области локтевых, тазобедренных, коленных и голеностопных суставов.
* При ощущении усталости глаз нужно в течение 2—3 мин. окинуть взглядом аудиторию (лабораторию), устремлять взгляд на разные предметы, смотреть вдаль (в окно).
1. Если резко возникло общее утомление, появилось дрожание изображения на экране дисплея (покачивание, подергивание, рябь), следует сообщить об этом преподавателю.
2. Выполнение практической работы должно происходить в соответствии с правилами выполнения практических работ (п. 4).

**7. ТЕМАТИКА ПРАКТИЧЕСКИХ РАБОТ И ЗАДАНИЯ К НИМ**

**Практическая работа 1 - 2.**

**Тема:** Разработка подсистемы защиты операционной системы Linux

**Цель занятия:** Получить навыки администрирования в операционной системе

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 4 часа.

**Задание:**

1. Создайте новую учетную запись пользователя.

1.1. В **Панели управления** выберите значок **Администрирование** и запустите оснастку **Управление компьютером.**

1.2. Откройте значок **Служебные программы** и выберите **Локальные пользователи и группы**.

1.3. Щелкните по **Пользователи** правой кнопкой мыши, и выберите меню **Новый пользователь**.

1.4. Задайте имя пользователя и его пароль входа в систему (пароль необходимо запомнить).

1.5. Нажмите кнопку **Создать.**

2. Настройте окружение пользователя.

2.1. Щелкните по имени пользователя правой кнопкой мыши и выберите  **Свойства**.

2.2. На закладке **Членство в группах** можно указать к каким группам пользователей принадлежит текущий пользователь, и, соответственно, какими правами этих групп он пользуется. Определите отсутствие принадлежности вашего пользователя к какой-либо группе.

2.3. Задайте домашний каталог пользователя. На закладке **Профиль** укажите путь к папке, где будут храниться индивидуальные файлы пользователя. Укажите локальный путь к папке.

3. Создайте вашу группу пользователей (Действия для ее создания аналогичны созданию новой учетной записи пользователя).

4. Назначение прав пользователям и группам. Создание пользователя не имеющего право локально регистрироваться на компьютере, но имеющего право получать доступ к его ресурсам из сети.

4.1. В оснастке **Администрирование** выберите **Локальная политика безопасности** – **Локальные политики – Назначение прав пользователя.** Найдите в колонке **Политика** право **Локальный вход в систему** и щелкнув в колонке **Локальный параметр** правой кнопкой мыши, выберите меню **Безопасность**. Посмотрите, кто из пользователей или групп пользователей имеет право на локальный вход. Чтобы ваш пользователь не имел права войти в систему локально, он не должен принадлежать к какой-либо группе в этом списке или быть явно указанным в нем. Кроме того он не должен принадлежать к группе **Все**. Настройте обладание этим правом таким образом, чтобы ваш пользователь мог локально зарегистрироваться на этом компьютере.

4.2. В списке прав найдите право **Доступ к компьютеру из сети**. Настройте это право таким образом, чтобы ваш пользователь обладал им.

4.3. Протестируйте локальный вход вашего пользователя на компьютер. Для этого завершите сеанс Администратора и попробуйте зарегистрироваться под именем вашего пользователя. Что при этом произойдет?

4.4. Протестируйте доступ вашего пользователя к компьютеру из сети. Для этого на другой машине создайте идентичную учетную запись, и зарегистрируйтесь на этой машине локально. Откройте значок сетевого окружения и попробуйте открыть какой-либо ресурс на первоначально настраиваемом вами компьютере.

5. Дайте вашему пользователю право локального входа в систему.

6. Создайте на диске С папку Test.

7. Настройте разрешения для этой папки.

7.1. Щелкните на ней правой кнопкой мыши и откройте ее **Свойства**.

7.2. Откройте закладку **Безопасность** и определите кто и какие разрешения имеет на доступ к папке.

7.3. Создайте еще три пользователя. В **безопасности** папки TEST первому пользователю дайте разрешение только на чтение этой папки, второму – на чтение и изменение, третьему – на полный контроль, четвертому – нет доступа.

7.4. Зарегистрируйтесь на машине последовательно под разными именами и попробуйте создавать, изменять и удалять файлы и папки внутри папки TEST.

8. Сделайте папку TEST общим (сетевым) ресурсом.

8.1. Откройте свойства папки TEST и выберите закладку **Доступ**.

8.2. Откройте общий доступ к этой папке и щелкнув по кнопке **Разрешения** определите возможности доступа к папке различных пользователей.

8.3. Протестируйте возможности доступа к созданному вами сетевому ресурсу с другого компьютера сети, зарегистрировавшись там под разными именами.

9. Создайте файл в папке TEST. Затем зарегистрируйтесь на компьютере под именем другого пользователя и сделайте так, чтобы он стал владельцем только, что созданного файла.

10. Установите и настройте аудит.

10.1. Откройте оснастку **Локальные политики** – **Политика аудита**.

10.2. Выберите пункт **Аудит доступа к объектам** и дважды щелкните на нем.

10.3. В появившемся диалоге выберите **Отказ**  и нажмите **Ок**. Тем самым вы включили аудит отказов при доступе в файлам, папкам, принтерам и т.д. Другими словами теперь в системе будут отслеживаться подобные события, и заноситься в журнал безопасности.

10.4. Откройте **свойства** папки TEST, закладку безопасность и нажмите кнопку **Дополнительно**.

10.5. В появившемся диалоге выберите закладку **Аудит**.

10.6. В список внесите имена тех пользователей, по отношению к которым будут отслеживаться события аудита. Добавьте в этот список пользователя, который не имеет разрешения на удаления файла из папки TEST.

10.7. Зарегистрируйтесь в системе от имени этого пользователя, и попробуйте удалить файл из папки TEST.

10.8. Войдите в систему от имени администратора и просмотрите журнал безопасности. Для этого откройте оснастку **Управление компьютером** и выберите пункт **Просмотр событий.** События аудита регистрируются в журнале безопасности.

10.9. Найдите в журнале событие об отказе удаления файла из папки TEST. Просмотрите сведения, щелкнув по нему дважды левой кнопкой мыши.

**Контрольные вопросы**

1. Как Linux различает пользователей?
2. В каких случаях следует применять профили?
3. Как создать домашнюю папку пользователя на другом компьютере (например, сервере)?
4. Как упростить создание большого количества пользователей?
5. Что такое ACL и как происходит наследование разрешений NTFS?

**Практическая работа 3 - 4.**

**Тема:** Реализация подсистемы защиты операционной системы Windows

**Цель занятия:** Получить навыки администрирования в операционной системе

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 4 часа.

**Задание:**

1. Создайте новую учетную запись пользователя.

1.1. В **Панели управления** выберите значок **Администрирование** и запустите оснастку **Управление компьютером.**

1.2. Откройте значок **Служебные программы** и выберите **Локальные пользователи и группы**.

1.3. Щелкните по **Пользователи** правой кнопкой мыши, и выберите меню **Новый пользователь**.

1.4. Задайте имя пользователя и его пароль входа в систему (пароль необходимо запомнить).

1.5. Нажмите кнопку **Создать.**

2. Настройте окружение пользователя.

2.1. Щелкните по имени пользователя правой кнопкой мыши и выберите  **Свойства**.

2.2. На закладке **Членство в группах** можно указать к каким группам пользователей принадлежит текущий пользователь, и, соответственно, какими правами этих групп он пользуется. Определите отсутствие принадлежности вашего пользователя к какой-либо группе.

2.3. Задайте домашний каталог пользователя. На закладке **Профиль** укажите путь к папке, где будут храниться индивидуальные файлы пользователя. Укажите локальный путь к папке.

3. Создайте вашу группу пользователей (Действия для ее создания аналогичны созданию новой учетной записи пользователя).

4. Назначение прав пользователям и группам. Создание пользователя не имеющего право локально регистрироваться на компьютере, но имеющего право получать доступ к его ресурсам из сети.

4.1. В оснастке **Администрирование** выберите **Локальная политика безопасности** – **Локальные политики – Назначение прав пользователя.** Найдите в колонке **Политика** право **Локальный вход в систему** и щелкнув в колонке **Локальный параметр** правой кнопкой мыши, выберите меню **Безопасность**. Посмотрите, кто из пользователей или групп пользователей имеет право на локальный вход. Чтобы ваш пользователь не имел права войти в систему локально, он не должен принадлежать к какой-либо группе в этом списке или быть явно указанным в нем. Кроме того он не должен принадлежать к группе **Все**. Настройте обладание этим правом таким образом, чтобы ваш пользователь мог локально зарегистрироваться на этом компьютере.

4.2. В списке прав найдите право **Доступ к компьютеру из сети**. Настройте это право таким образом, чтобы ваш пользователь обладал им.

4.3. Протестируйте локальный вход вашего пользователя на компьютер. Для этого завершите сеанс Администратора и попробуйте зарегистрироваться под именем вашего пользователя. Что при этом произойдет?

4.4. Протестируйте доступ вашего пользователя к компьютеру из сети. Для этого на другой машине создайте идентичную учетную запись, и зарегистрируйтесь на этой машине локально. Откройте значок сетевого окружения и попробуйте открыть какой-либо ресурс на первоначально настраиваемом вами компьютере.

5. Дайте вашему пользователю право локального входа в систему.

6. Создайте на диске С папку Test.

7. Настройте разрешения для этой папки.

7.1. Щелкните на ней правой кнопкой мыши и откройте ее **Свойства**.

7.2. Откройте закладку **Безопасность** и определите кто и какие разрешения имеет на доступ к папке.

7.3. Создайте еще три пользователя. В **безопасности** папки TEST первому пользователю дайте разрешение только на чтение этой папки, второму – на чтение и изменение, третьему – на полный контроль, четвертому – нет доступа.

7.4. Зарегистрируйтесь на машине последовательно под разными именами и попробуйте создавать, изменять и удалять файлы и папки внутри папки TEST.

8. Сделайте папку TEST общим (сетевым) ресурсом.

8.1. Откройте свойства папки TEST и выберите закладку **Доступ**.

8.2. Откройте общий доступ к этой папке и щелкнув по кнопке **Разрешения** определите возможности доступа к папке различных пользователей.

8.3. Протестируйте возможности доступа к созданному вами сетевому ресурсу с другого компьютера сети, зарегистрировавшись там под разными именами.

9. Создайте файл в папке TEST. Затем зарегистрируйтесь на компьютере под именем другого пользователя и сделайте так, чтобы он стал владельцем только, что созданного файла.

10. Установите и настройте аудит.

10.1. Откройте оснастку **Локальные политики** – **Политика аудита**.

10.2. Выберите пункт **Аудит доступа к объектам** и дважды щелкните на нем.

10.3. В появившемся диалоге выберите **Отказ**  и нажмите **Ок**. Тем самым вы включили аудит отказов при доступе в файлам, папкам, принтерам и т.д. Другими словами теперь в системе будут отслеживаться подобные события, и заноситься в журнал безопасности.

10.4. Откройте **свойства** папки TEST, закладку безопасность и нажмите кнопку **Дополнительно**.

10.5. В появившемся диалоге выберите закладку **Аудит**.

10.6. В список внесите имена тех пользователей, по отношению к которым будут отслеживаться события аудита. Добавьте в этот список пользователя, который не имеет разрешения на удаления файла из папки TEST.

10.7. Зарегистрируйтесь в системе от имени этого пользователя, и попробуйте удалить файл из папки TEST.

10.8. Войдите в систему от имени администратора и просмотрите журнал безопасности. Для этого откройте оснастку **Управление компьютером** и выберите пункт **Просмотр событий.** События аудита регистрируются в журнале безопасности.

10.9. Найдите в журнале событие об отказе удаления файла из папки TEST. Просмотрите сведения, щелкнув по нему дважды левой кнопкой мыши.

**Контрольные вопросы**

1. Как Windows 2000 различает пользователей?
2. В каких случаях следует применять профили?
3. Как создать домашнюю папку пользователя на другом компьютере (например, сервере)?
4. Как упростить создание большого количества пользователей?
5. Что такое ACL и как происходит наследование разрешений NTFS?

**Практическое занятие** **5**

**Тема:** Обеспечение защиты вычислительной сети

**Цель занятия:** получение практических навыков при работе с консолью управления MMC, научиться создавать расписание запуска заданий при помощи Планировщика заданий

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 2 часа.

**Задание:**

*Создайте пользовательскую консоль. Затем с помощью созданной консоли определите время последнего запуска компьютера. Добавьте в консоль оснастку с расширениями.*

**Задание№1: создайте пользовательскую консоль**

1. В меню *Пуск* выберите команду *Выполнить*.
2. В поле *Открыть* введите **mmc** и щелкните ОК.
MMC выведет на экран пустую консоль.
3. Разверните окно *Консоль1* на весь экран.
4. Разверните окно *Корень консоли* на все окно MMC
5. Чтобы просмотреть текущие параметры консоли, в меню *Консоль* выберите команду *Параметры*.
Заметьте, что по умолчанию используется авторский режим консоли. Помните, что данный режим предоставляет пользователям полный доступ ко всей функциональности MMC.
6. Убедитесь, что в списке *Режим консоли* выбран пункт *Авторский режим* и щелкните ОК.
7. В меню *Консоль* выберите команду *Добавить/удалить оснастку*
Откроется одноименное диалоговое окно.
8. Щелкните кнопку Добавить.
Откроется диалоговое окно *Добавить Изолированную оснастку*
Обратите внимание на список доступных оснасток. ММС позволяет добавлять в консоль оснастки и создавать таким образом собственные средства управления.
9. Выберите *Управление компьютером* и щелкните кнопку Добавить. Откроется одноименное диалоговое окно.
10. Шелкните переключатель *Локальный компьютер:(Консоль того компьютера, на. котором выполняется эта консоль),* а затем — кнопку Готово.
В окне (*добавить/удалить оснастку)* появился элемент *Управление компьютером (локальным*)
11. Щелкните *Закрыть*, чтобы закрыть диалоговое окно
12. В меню (*Консоль*) выберите команду (*Сохранить как*)
Откроется одноименное диалоговое окно.
13. В поле (*Имя файла*) введите *All Event* и шелкните кнопку *Save*
имя созданной консоли появится в заголовке окна ММС.

**Задание №2: проверьте местоположение пользовательской консоли**

*Убедитесь, что консоль сохранена в папке Административные средства — закройте и повторно откройте созданную консоль.*

1. В меню (*Консоль*) выберите команду (*Выход*).
На данный момент вы создали и сохранили пользовательскую консоль *All Events*.
2. в меню (*Пуск*) выберите команду (*Выполнить*). В поле (*Открыть*) введите **mmc** и щелкните ОК.
3. в меню Консоль выберите команду (*Открыть*). Откроется одноименное диалоговое окно. Заметьте, что созданная консоль (*All Events.msc*) находится в папке *Административные средства*.
4. Выберите файл *All Events* и щелкните кнопку *Открыть*. Windows XP откроет консоль *All Events*

**Контрольные вопросы:**

1. Когда и для чего применяются расширения?
2. Вам необходимо создать пользовательскую консоль для администратора, которому требуются лишь оснастки Управление компьютером и Active Directory — пользователи и компьютеры. Какой режим следует выбрать при сохранении пользовательской консоли если...
а) ...у администратора не должно быть прав на добавление дополнительных оснасток?
б) ...администратору требуется полный доступ к обеим оснасткам.
в) администратору требуется возможность переключения между оснастками.
3. Что сделать для удаленного администрирования компьютера Windows Server с компьютера Windows XP?
4. На вашем компьютере с Windows XP раз в неделю должна автоматически запускаться одна из служебных программ. Как этого добиться?

**Практическое занятие** **6**

**Тема:** Управление доступом в операционных системах

**Цель занятия:** изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 2 часа.

**Задание:**

1. Запустите виртуальную ма­шину WinXP. Войдите в систему под учетной записью администратора,. Все действия в пп 2.2.1-2.2.8 выполняйте в системе, рабо­тающей на виртуальной машине.

2. Создайте учетную запись нового пользователя testUser в оснаст­ке «Управление компьютером» (compmgmt.msc). При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок дей­ствия его пароля. Создайте новую группу ”testGroup” и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске С: папку forTesting. Создайте или скопируйте в эту папку несколько текстовых файлов (\*.txt).

3. С помощью команды runas запустите сеанс командной строки

(cmd.exe) от имени вновь созданного пользователя. Командой whoami посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя.

Строку запуска и результат работы этой и всех следующих консольных команд копируйте в файл протокола лабораторной работы.

4. Убедитесь в соответствии имени пользователя и полученного SID

в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен SID S-1-5-21-1957994488-492894223-170857768-1004 (Используйте ключ реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList).

5. Командой whoami определите перечень текущих привилегий пользователя testUser. В сеансе командной строки пользователя попробуйте изме­нить системное время командой time. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «Локальные параметры безопасности» (secpol.msc). Добавьте пользователя в список параметров политики «Изменение системного времени» раздела Локальные политики -> Назначение прав поль­зователя. После этого перезапустите сеанс командной строки от имени пользова­теля, убедитесь, что в списке привилегий добавилась SeSystemtimePriviege. По­пробуйте изменить системное время командой time.

Убедитесь, что привилегия «Завершение работы системы» (SeShutdownPrivilege) предоставлена пользователю testUser . После этого попро­буйте завершить работу системы из сеанса командной строки пользователя коман­дой shutdown -s. Добавть ему привелегию «Принудительное удаленное завер­шение» (SeRemoteShutdownPrivilege). Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выпол­нения можно командой shutdown -а).

**Контрольные вопросы**

1. К какому классу безопасности относится ОС Windows по различным критериям оценки?
2. Каким образом пользователи идентифицируются в ОС Windows?
3. Что такое списки DACL и SACL?
4. Перечислите, каким образом можно запустить процесс от имени друго­го пользователя.

**Практическое занятие** **7**

**Тема:** Идентификация и аутентификация пользователей операционных систем

**Цель занятия:** изучить модель безопасности операционной системы Windows, получить навыки практического использования идентификация и аутентификация пользователей операционных систем

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 2 часа.

**Ход проведения занятия:**

Ознакомьтесь с справкой по консольной команде cacls. Используя эту команду, просмотрите разрешения на папку c:\forTesting. Объясните все обозначе­ния в описаниях прав пользователей и групп в выдаче команды.

а) Разрешите пользователю testUser запись в папку forTesting, но запретите запись для группы testGroup. Попробуйте записать файлы или папки в forTesting от имени пользователя testUser. Объясните результат. Посмотрите эффективные разрешения пользователя testUser к папке forTesting в окне свойств папки.

б) Используя стандартное окно свойств папки, задайте для пользователя testUser такие права доступа к папке, чтобы он мог записывать информацию в пап­ку forTesting, но не мог просматривать ее содержимое. Проверьте, что папка forTesting является теперь для пользователя testUser “слепой”, запустив, напри­мер, от его имени файловый менеджер и попробовав записать файлы в папку, про­смотреть ее содержимое, удалить файл из папки.

в) Для вложенной папки forTesting\Docs отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка forTesting\Docs перестала быть “слепой” (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл).

г) Снимите запрет на чтение папки forTesting для пользователя testUser. Используя команду cacls запретите этому пользователю доступ к файлам с расши­рением txt в папке forTesting. Убедитесь в недоступности файлов для пользовате­ля.

д) Командой cacls запретите пользователю все права на доступ к папке forTesting и разреште полный доступ к вложенной папке forTesting\Docs. Убеди­тесь в доступности папки forTesting\Docs для пользователя. Удалите у пользовате­ля testUser привилегию SeChangeNotifyPrivilege. Попробуйте получить доступ к папке forTesting\Docs. Объясните результат.

е) Запустите файловый менеджер от имени пользователя testUser и создайте в нем папку newFolder на диске C. Для папки newFolder очистите весь список ACL командой cacls. Попробуйте теперь получить доступ к папке от имени адми­нистратора и от имени пользователя. Кто и как теперь может вернуть доступ к пап­ке? Верните полный доступ к папке для всех пользователей.

ж) Создайте в разделе HKLM\Software реестра раздел testKey. Запретите пользователю testUser создание новых разделов в этом разделе реестра. Создайте для раздела HKLM\Software\testKey SACL, позволяющий протоколировать отка­зы при создании новых подразделов, а также успехи при перечислении подразде­лов и запросе значений (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита включен). Попробуйте от имени поль­зователя testUser запустить regedit.exe и создать раздел в HKLM\Software. Убеди­тесь, что записи аудита были размещены в журнале безопасности (eventvwr.msc).

**Контрольные вопросы**

1. Как с использованием команды cacls добавить права на запись для всех файлов заданной папки?
2. Какие события подлежат аудиту в ОС Windows?
3. Каким образом шифруются файлы в файловой системе EFS?
4. Какие алгоритмы шифрования используются в EFS?

**Практическое занятие 8**

**Тема:** Организация защиты данных СУБД SQL Server 2008

**Цель занятия:** получить навыки построения защиты БД

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 2 часа.

**Задание:Построить защиту данных**

**Ход проведения занятия:**

1. Запустить сервер MySQL. Идем в системное меню Пуск - Программы - MySQL - MySQL Server 5.1 - MySQL Command Line Client. Откроется окно, предлагающее ввести пароль.

Нажимаем Enter на клавиатуре, если вы не указывали пароль при настройке сервера или указываем пароль, если вы его задавали. Ждем приглашения mysql>.

Нам надо создать базу данных, которую мы назовем forum. Для этого в SQL существует оператор *create database*. Создание базы данных имеет следующий синтаксис:

create database имя\_базы\_данных;

Максимальная длина имени БД составляет 64 знака и может включать буквы, цифры, символ "\_" и символ "$". Имя может начинаться с цифры, но не должно полностью состоять из цифр. Любой запрос к БД заканчивается точкой с запятой (этот символ называется разделителем - delimiter). Получив запрос, сервер выполняет его и в случае успеха выдает сообщение "Query OK ..."

2. Создадим БД forum:



Нажимаем Enter и видим ответ "Query OK ...", означающий, что БД была создана:



Вот так все просто. Теперь в этой базе данных нам надо создать 3 таблицы: темы, пользователи и сообщения. Но перед тем, как это делать, нам надо указать серверу в какую именно БД мы создаем таблицы, т.е. надо выбрать БД для работы. Для этого используется оператор *use*. Синтаксис выбора БД для работы следующий:

use имя\_базы\_данных;

3.Выберем для работы нашу БД forum:



Нажимаем Enter и видим ответ "Database changed" - база данных выбрана.



Выбирать БД необходимо в каждом сеансе работы с MySQL.

Для создания таблиц в SQL существует оператор *create table*. Создание базы данных имеет следующий синтаксис:

create table имя\_таблицы (имя\_первого\_столбца тип, имя\_второго\_столбца тип, ..., имя\_последнего\_столбца тип );

4. Требования к именам таблиц и столбцов такие же, как и для имен БД. К каждому столбцу привязан определенный тип данных, который ограничивает характер информации, которую можно хранить в столбце (например, предотвращает ввод букв в числовое поле). MySQL поддерживает несколько типов данных: числовые, строковые, календарные и специальный тип NULL, обозначающий отсутствие информации. Подробно о типах данных мы будем говорить в следующем уроке, а пока вернемся к нашим таблицам. В них у нас всего два типа данных - целочисленные значения (int) и строки (text). Итак, создадим первую таблицу - Темы:



Нажимаем Enter - таблица создана:



Итак, мы создали таблицу topics (темы) с тремя столбцами:
id\_topic int - id темы (целочисленное значение),
topic\_name text - имя темы (строка),
id\_author int - id автора (целочисленное значение).

Аналогичным образом создадим оставшиеся две таблицы - users (пользователи) и posts (сообщения):



Итак, мы создали БД forum и в ней три таблицы. Сейчас мы об этом помним, но если наша БД будет очень большой, то удержать в голове названия всех таблиц и столбцов просто невозможно. Поэтому надо иметь возможность посмотреть, какие БД у нас существуют, какие таблицы в них присутствуют, и какие столбцы эти таблицы содержат. Для этого в SQL существует несколько операторов:
*show databases* - показать все имеющиеся БД,
*show tables* - показать список таблиц текущей БД (предварительно ее надо выбрать с помощью оператора *use*),
*describe имя\_таблицы* - показать описание столбцов указанной таблицы.

Давайте попробуем. Смотрим все имеющиеся базы данных



Теперь посмотрим список таблиц БД forum (для этого ее предварительно надо выбрать), не забываем после каждого запроса нажимать Enter:



В ответе видим названия наших трех таблиц. Теперь посмотрим описание столбцов, например, таблицы topics:



Первые два столбца нам знакомы - это имя и тип данных, значения остальных нам еще предстоит узнать. Но прежде мы все-таки узнаем какие типы данных бывают, какие и когда следует использовать.

5. Рассмотрим последний оператор - *drop*, он позволяет удалять таблицы и БД. Например, давайте удалим таблицу topics. Так как мы два шага назад выбирали БД forum для работы, то сейчас ее выбирать не надо, можно просто написать:

drop table имя\_таблицы;

и нажать Enter.



Теперь снова посмотрим список таблиц нашей БД:



Наша таблица действительно удалена. Теперь давайте удалим и саму БД forum (удаляйте, не жалейте, ее все равно придется переделывать). Для этого напишем:

drop database имя\_базы данных;

и нажмем Enter.



И убедитесь в этом, сделав запрос на все имеющиеся БД:

**Контрольные вопросы:**

1. Для чего необходимы операторы в БД.

2. Приведите пример операторов.

**Практическое занятие 9**

**Тема:** Создание Web страниц.

**Цель занятия:** Знакомство с общими положениями создания WEB-страниц и базовыми тегами языка HTML

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 2 часа.

**Задание:**

1. Создайте стандартный текстовый файл.

2. Откройте его редактором "Блокнот".

3. Сначала напечатайте основные теги:
<HTML>
<HEAD>
<TITLE>Добро пожаловать !!!</TITLE>
</HEAD>
<BODY> Здравствуйте!!!
</BODY>
</HTML>

4. Сохраните документ с расширением \*.htm.

5. Создайте веб-страницу с оформленным фоном и текстом.

HTML-код будет выглядеть следующим образом:

<HTML>
<BODY BACKGROUND="paint1.bmp" BGCOLOR="red" TEXT="cian" LEFTMARGIN="40" MARGINWIDTH="40">
...
Текст документа (5-6 предложений на любую тему).
...
</BODY>
</HTML>

6. Сохраните документ с расширением \*.htm.

Самостоятельно создайте две веб-страницы с разными фонами и цветами текстов (5-6 предложений).

**Практическое занятие 10**

**Тема:** Создание БД Access с помощью SQL

**Цель занятия:** Получить навыки создания БД

**Оснащение рабочего места:** Персональный компьютер

**Продолжительность занятия** – 2 часа.

**Задание:**

1. Мы познакомились с типами данных, теперь будем усовершенствовать таблицы для нашего форума. Сначала разберем их. И начнем с таблицы users (пользователи). В ней у нас 4 столбца:

id\_user - целочисленные значения, значит будет тип int, ограничим его 10 символами - int (10).
name - строковое значение varchar, ограничим его 20 символами - varchar(20).
email - строковое значение varchar, ограничим его 50 символами - varchar(50).
password - строковое значение varchar, ограничим его 15 символами - varchar(15).

Все значения полей обязательны для заполнения, значит надо добавить тип NOT NULL.

id\_user int (10) NOT NULL
name varchar(20) NOT NULL
email varchar(50) NOT NULL
password varchar(15) NOT NULL

Первый столбец, как вы помните из концептуальной модели нашей БД, является первичным ключом (т.е. его значения уникальны, и они однозначно идентифицируют запись). Следить за уникальностью самостоятельно можно, но не рационально. Для этого в SQL есть специальный атрибут - *AUTO\_INCREMENT*, который при обращении к таблице на добавление данных высчитывает максимальное значение этого столбца, полученное значение увеличивает на 1 и заносит его в столбец. Таким образом, в этом столбце автоматически генерируется уникальный номер, а следовательно тип NOT NULL излишен. Итак, присвоим атрибут столбцу с первичным ключом:

id\_user int (10) AUTO\_INCREMENT
name varchar(20) NOT NULL
email varchar(50) NOT NULL
password varchar(15) NOT NULL

2. Теперь надо указать, что поле id\_user является первичным ключом. Для этого в SQL используется ключевое слово *PRIMARY KEY ()*, в скобочках указывается имя ключевого поля. Внесем изменения:

id\_user int (10) AUTO\_INCREMENT
name varchar(20) NOT NULL
email varchar(50) NOT NULL
password varchar(15) NOT NULL
PRIMARY KEY (id\_user)

Итак, таблица готова, и ее окончательный вариант выглядит так:

create table users (
id\_user int (10) AUTO\_INCREMENT,
name varchar(20) NOT NULL,
email varchar(50) NOT NULL,
password varchar(15) NOT NULL,
PRIMARY KEY (id\_user)
);

3. Теперь разберемся со второй таблицей - topics (темы). Рассуждая аналогично, имеем следующие поля:

id\_topic int (10) AUTO\_INCREMENT
topic\_name varchar(100) NOT NULL
id\_author int (10) NOT NULL
PRIMARY KEY (id\_topic)

Но в модели нашей БД поле id\_author является внешним ключом, т.е. оно может иметь только те значения, которые есть в поле id\_user таблицы users. Для того, чтобы указать это в SQL есть ключевое слово *FOREIGN KEY ()*, которое имеет следующий синтаксис:

FOREIGN KEY (имя\_столбца\_которое\_является\_внешним\_ключом) REFERENCES имя\_таблицы\_родителя (имя\_столбца\_родителя);

Укажем, что id\_author - внешний ключ:

id\_topic int (10) AUTO\_INCREMENT
topic\_name varchar(100) NOT NULL
id\_author int (10) NOT NULL
PRIMARY KEY (id\_topic)
FOREIGN KEY (id\_author) REFERENCES users (id\_user)

Таблица готова, и ее окончательный вариант выглядит так:

create table topics (
id\_topic int (10) AUTO\_INCREMENT,
topic\_name varchar(100) NOT NULL,
id\_author int (10) NOT NULL,
PRIMARY KEY (id\_topic),
FOREIGN KEY (id\_author) REFERENCES users (id\_user)
);

4. Осталась последняя таблица - posts (сообщения). Здесь все аналогично, только два внешних ключа:

create table posts (
id\_post int (10) AUTO\_INCREMENT,
message text NOT NULL,
id\_author int (10) NOT NULL,
id\_topic int (10) NOT NULL,
PRIMARY KEY (id\_post),
FOREIGN KEY (id\_author) REFERENCES users (id\_user),
FOREIGN KEY (id\_topic) REFERENCES topics (id\_topic)
);

5. Обратите внимание, внешних ключей у таблицы может быть несколько, а первичный ключ в MySQL может быть только один. В первом уроке мы удалили нашу БД forum, пришло время создать ее вновь.

**8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ МДК**

**Основные источники (ОИ):**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Автор | Издательство, год издания |
| ОИ 1 | Организация комплексной системы защиты информации | Гришина Н.В | М.: Гелиос АРВ, 2010 |
| ОИ 2 | Информационная безопасность: 3-е издание | Мельников В.П. | М: Издательский центр «Академия», 2010 |
| ОИ 3 | Информационная безопасность предприятия  | Конеев И. Р. | СПб.: БХВ-Петербург, 2010 |

**Дополнительные источники (ДИ):**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Автор | Издательство, год издания |
| ДИ 1 | Комплексная система защиты информации на предприятии | Гришина Н. В. | М.: Форум, 2009. |
| ДИ 2 | Защита информации в персональном компьютере: учебное пособие | Емельянова Н.З., Партыка Т.Л., Попов И.И. | М.: Форум, 2009. |
| ДИ 3 | Основы информационной безопасности: учебное пособие | Галатенко В.А. | Интернет-Университет Информационных Технологий, www.intuit.ru, 2010. |

**Интернет-ресурсы (ИР):**

|  |  |
| --- | --- |
| ИР 1 | http://window.edu.ru/ |
| ИР 2 | <http://inf.1september.ru/> |
| ИР 3 | http://www.informsviaz.ru/inform\_tech/617.html |
| ИР 4 | http://www.metodist.ru/ |
| ИР 5 | http://metodist.lbz.ru/ |