МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению самостоятельных работ
по дисциплине

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки	10.03.01 Информационная безопасность
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

ВВЕДЕНИЕ

Методические указания содержат курс самостоятельных работ по дисциплине «Основы управления информационной безопасностью» направленный на изучение принципов функционирования и элементной базы вычислительных систем.

Содержащиеся в данном пособии сведения теории, методические указания и рекомендации по выполнению самостоятельных работ позволяют использовать его в качестве дополнительного пособия для закрепления курса лекций.

Методические рекомендации для студентов по изучению дисциплины

1.1. Использование материала учебно-методического комплекса дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с практическими и лабораторными занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов
ОК-5, ОПК-7	Изучение литературы по темам № 3, 6, 7, 12	Конспект	Собеседование.	20
ПК-3,4,5,6,13,14,15	Подготовка к практическому занятию	Индивидуальное задание	Письменный отчет.	40
			Итого за 8 семестр	**60**

1.2.Работа с литературой

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополни-тельная	Методи-ческая	Интернет-ресурсы
1	Тема 3. Морально этические нормы защиты информации на предприятии.	1,2	1,2,3	1,2	1,2,3
2	Тема 6. Процесс оценки риска информационной безопасности.	1,2	1,2,3	1,2	1,2,3
3	Тема 7. Идентификация уязвимостей и построение модели нарушителя.	1,2	1,2,3	1,2	1,2,3
4	Тема 12. Построение структурного подразделения информационной безопасности.	1,2	1,2,3	1,2	1,2,3

2. Примерная тематика заданий для самостоятельной работы студентов

1. Нормативная правовая база информационной безопасности РФ.
2. Становление концептуальных правовых основ информационной безопасности в РФ.
3. Информационные технологии и право.
4. Национальные интересы Российской Федерации в информационной сфере.
5. Состояние информационной безопасности Российской Федерации.
6. Государственная политика обеспечения информационной безопасности РФ.
7. Информация как объект правового регулирования.
8. Правовые основы информационной безопасности личности.

9. Государственная тайна – элемент информационной безопасности государства.
10. Опасности, подстерегающие пользователя в сети Интернет.
11. Спам – чума XXI века.
12. Оптимизация работы операционной системы.
13. Восстановление информации.
14. Электронные цифровые подписи – новый метод обеспечения информационной безопасности государства.
15. Компьютерные вирусы и их свойства
16. Антивирусные программы.
17. Проактивные системы защиты и системы контроля целостности.
18. Системы отражения атак.
19. Блокирование несанкционированного доступа к компьютеру.
20. Анонимность пользователя в сети Интернет.
21. Комплексная бесплатная защита компьютера.
22. В поисках правильного пароля.
23. Шифрование информации.
24. Аналитическая работа как основа формирования системы защиты информации.
25. Организация работы с персоналом, обладающим конфиденциальной информацией.
26. Ребенок и компьютер.
27. Принцип сохранения данных путем создания резервных копий. Виды Архиваторов и принципы их работы.
28. Защита личных имущественных и неимущественных прав личности в информационной сфере.
29. Профессиональные тайны как подсистема информационной безопасности личности.
30. СМИ как объект информационной безопасности современного общества.

3 Рекомендуемая литература.

3.1 Основная литература:

1. Сергеева Ю.С. Защита информации. Конспект лекций. – М.: А-Приор, 2011.
2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

3.2. Дополнительная литература:

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2008.
2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2008.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб.пособие/ В.Ф. Шаньгин – М.: ФОРУМ, 2008.

3.3 Методическая литература:

1. Методические указания по выполнению практических работ по дисциплине «Управление информационной безопасностью» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения. Пятигорск, 2017.
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Управление информационной безопасностью» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения. Пятигорск, 2017.

3.4 Интернет-ресурсы:

1. http://www.intuit.ru/department/ds/discrmath - Интернет университет информационных технологий;
2. http://www.studfiles.ru/dir/cat14/subj266/file4146/view34225.html - StudFiles. Все для учебы;
3. http://lib.mexmat.ru/indsearch.php - Электронная библиотека механико-математического факультета МГУ.

3.5 Программное обеспечение:

1. Программное обеспечение для защиты от несанкционированного доступа SecretNet 2000/XP/2003, v 5.0.
2. Microsoft Office System 2007, 2010
3. Microsoft Virtual PC.

4. Материально-техническое обеспечение дисциплины:

Лаборатория информационной безопасности

1. 12 компьютеров IBMPCPentium 4.
2. Детекторы электромагнитного излучения.
3. Сканер электромагнитного излучения.
4. Приборы измерения параметров акустических сигналов.
5. Оборудование защиты телефонных линий от утечки сигналов.
6. ПО криптографической защиты информации.
7. Оборудование для скремблирования сигналов.
8. Средства для инженерно-технической защиты информации.
9. Стенд лабораторный «ПКП MagnumAlert+клавиатура».
10. Стенд лабораторный «ПКП Summit 3208+клавиатура».
11. Стенд лабораторный «ПКП 9234+».
12. Извещатели различных типов (12 шт).
13. Устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН “Соната-РК1”.
14. Имитаторы закладных устройств «Шиповник-2» и «ИМФ-2».
15. Скоростной поисковый приемник «Скорпион v.34».
16. Электронно-оптическое устройство «Оптик».
17. Индикатор поля «Карточка» «SEL SP – 75».
18. Портативный металлодетектор «Сфинкс» «ВМ – 612» (в составе: аккумулятор, ЗУ, виброиндикация).
19. Генератор-излучатель акустического шума «СА-65/М».
20. Генератор-излучатель виброакустического шума «СВ-45/М».
21. Генератор шума «ГШ-2500».
22. Генератор шума по сети электропитания и линиям заземления «Соната – РС 1».