


ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



УТВЕРЖДАЮ:

Проректор по научно-педагогической работе

 (подпись) А. В. Левшов И.О. Фамилия

« 03 » 07 20 17 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Управление информационной безопасностью»
(наименование дисциплины согласно учебному плану)

Направление (специальность)
подготовки:

10.03.01 «Информационная безопасность»
(код и наименование направления / специальности)

Направленность:

Информационная безопасность
(наименование профиля / магистерской программы / специализации)

Уровень образования:

бакалавриат

(бакалавриат, магистратура, специалитет)

Форма обучения:

очная

(очная, заочная, очно-заочная)

Семестры	7
Общая трудоёмкость в з.е./часах	2,5/90
Аудиторные занятия (час.), в том числе	51
Лекции (час.)	34
Практические (семинарские) занятия (час.)	-
Лабораторные работы (час.)	17
Самостоятельная работа (час.), в том числе	39
Курсовой проект/работа (сем/кол.)	-
Индивидуальное задание (сем/кол.)	1
Форма промежуточной аттестации (экзамен/зачёт):	Зачет

Донецк, 2017 г.

Рабочая программа дисциплины Управление информационной безопасностью составлена в соответствии с учебным планом по направлению подготовки 10.03.01 «Информационная безопасность» для бакалавриата профиля «Информационная безопасность» для 2017 года приёма.

Составитель: Якушина А.Е., ст. преподаватель кафедры «Радиотехника и защита информации».

Рабочая программа **рассмотрена и принята** на заседании кафедры «Радиотехника и защита информации».

Протокол от «25» 05 2017 года № 5

Заведующий кафедрой _____ Паслен В. В.

Рабочая программа **согласована с выпускающей кафедрой** «Радиотехника и защита информации».

Протокол от «25» 05 20 17 года № 5

Заведующий кафедрой _____ Паслен В. В.

Рабочая программа **одобрена учебно-методической комиссией** ДонНТУ по направлению подготовки 10.03.01 «Информационная безопасность».

Протокол от «30» 06 20 17 года № 5

Председатель _____ Паслен В. В.

Рабочая программа **продлена** для 20 18 года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от « 31 » 08 20 18 года № 1
Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой «Радиотехника и защита информации».

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20 19 года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от « 28 » 08 20 19 года № 1
Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой «Радиотехника и защита информации».

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20 ____ года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от « ____ » ____ 20 ____ года № ____
Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой «Радиотехника и защита информации».

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

1. ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель и задачи дисциплины.

Сформировать у студентов знания и навыки по подбору, изучению и обобщению национальных и международных стандартов, научно-технической литературы, нормативных и методических материалов; составлению обзора по вопросам обеспечения информационной безопасности в автоматизированных информационных системах; управлению информационной безопасностью.

В результате освоения дисциплины студент должен:

- знать: основы управления информационной безопасностью; основные требования международных и национальных стандартов по управлению информационной безопасностью; правила управления информационной безопасностью; основные документы политики информационной безопасности; содержание и порядок выполнения работ на стадиях и этапах создания системы комплексной защиты информации (СКЗИ) организации (предприятия); цели, задачи и структуру службы защиты информации организации (предприятия); основы конфиденциального делопроизводства;

- уметь: проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; формировать комплекс мер по обеспечению информационной безопасности; разрабатывать основные документы политики информационной безопасности; оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.

Перечисленные результаты обучения являются основой для формирования следующих компетенций: ОК-6, ОК-7, ОК-10, ОПК-1, ОПК-2, ОПК-4, ОПК-5, ОПК-7, ОПК-8, ОПК-10, ПК-5, ПК-6, ПК-8, ПК-10, ПК-12, ПК-13, ПК-17, ПК-18, ПК-21, ПК-22, ПК-25.

2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к профессиональному циклу вариативной части дисциплин по выбору вуза учебного плана.

Базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин: организационное обеспечение технической защиты информации, методы и средства защиты информации.

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при изучении последующих дисциплин: «Проектирование систем защиты информации», «Организационное обеспечение технической защиты информации», при выполнении и защите бакалаврской работы, а также – в последующей профессиональной деятельности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Распределение учебных часов по темам дисциплины и видам занятий

Наименование тем (содержательных модулей)	Количество часов				
	Всего	В том числе			
		Лекции	Практ. (Семина.)	Лабор.	СРС
Тема 1. Основные понятия информационной безопасности	4	2	-	1	4
Тема 2. Угрозы информационной безопасности в информационных системах	10	4	-	2	5
Тема 3. Оценочные стандарты в информационной безопасности.	8	4	-	2	5
Тема 4. Стандарты управления информационной безопасностью	10	4	-	2	5
Тема 5. Создание СУИБ на предприятии	14	6	-	4	5
Тема 6. Методики оценки рисков информационной безопасности компании	12	6	-	2	5
Тема 7. Правовые меры обеспечения информационной безопасности	10	4	-	2	5
Тема 8. Организационные меры обеспечения безопасности компьютерных информационных систем	10	4	-	2	5
Итого:	90	34	-	17	39

3.2. Лекции

Тема 1. Основные понятия информационной безопасности

Содержание темы 1:

Понятие информационной безопасности. Объект защиты информации. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности.

Литература к теме 1: [1, 2]

Тема 2. Угрозы информационной безопасности в информационных системах

Содержание темы 2:

Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредительские программы.

Литература к теме 2: [1, 2,3]

Тема 3. Оценочные стандарты в информационной безопасности. Содержание темы 3:

Роль стандартов ИБ. «Оранжевая книга» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Литература к теме 3: [1, 2,3]

Тема 4. Стандарты управления информационной безопасностью

Содержание темы 4:

Стандарты управления информационной безопасностью. BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.

Литература к теме 4: [1, 2,3]

Тема 5. Создание СУИБ на предприятии

Содержание темы 5:

Этапы создания системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков.

Литература к теме 5: [1, 2, 3]

Тема 6. Методика оценки рисков информационной безопасности компании

Содержание темы 6:

Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей. Методика оценки рисков информационной безопасности компании Digital Security. Методики и технологии управления рисками. Разработка корпоративной методики анализа рисков.

Литература к теме 6: [1, 2, 3]

Тема 7. Правовые меры обеспечения информационной безопасности

Содержание темы 7:

Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.

Литература к теме 7: [1, 2, 3]

Тема 8. Организационные меры обеспечения безопасности компьютерных информационных систем

Содержание темы 8:

Общие положения организационной защиты. Особенности организационной защиты компьютерных информационных систем и сетей. Служба безопасности предприятия.

Литература к теме 8: [1, 2, 3]

3.3. Лабораторные занятия

№ п/п	Тема занятия	Объем, час.	Литература
1	Сбор данных об информационной системе с помощью средств администрирования Windows (оснасток MMC)	2	[1-3]
2	Сбор данных о топологии сети с помощью средства	2	[1-3]

	администрирования сетей 3Com Network Supervisor		
3	Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer. Настройка локальной политики паролей	2	[1-3]
4	Использование сканеров безопасности для получения информации о сети.	2	[1-3]
5	Реализация дискреционной модели политики безопасности	2	[1-3]
6	Количественная оценка стойкости парольной защиты	2	[1-3]
7	Ассиметричные алгоритмы шифрования данных	2	[1-3]
8	Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра	2	[1-3]
Итого:		17	

3.4. Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час.
1	Изучение лекционного материала (не менее 50% от объема лекций)	17
2	Подготовка к лабораторным занятиям (не менее 50% от объема аудиторных практических занятий)	22
Итого:		39

3.5. Курсовой проект (работа), индивидуальное задание

Курсовой проект (работа) по дисциплине учебным планом не предусмотрен.

Объем учебной нагрузки при выполнении одного индивидуального задания – не менее 9 часов.

Рекомендуемый объем пояснительной записки по индивидуальному заданию – не более 12 страниц формата А4 (210×297 мм).

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Текущий контроль знаний студентов производится по результатам выполнения лабораторных работ, индивидуального задания.

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового зачета в соответствии с «Положением об организации учебного процесса в Донецком национальном техническом университете (новая редакция)», утвержденном приказом ДонНТУ № 1006-14 от 01.12.2016г.

Для определения уровня знаний студентов преподаватель руководствуется критериями оценки знаний, являющимися составляющей учебно-методического комплекса дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Литература:

Учебная литература:

Основная:

1. Мельников, В.П. Исследование систем управления / В. П. Мельников. - М. : ИЦ "Академия", 2008. - 336с. - 2 экз.
2. Грушо, А.А. Теоретические основы компьютерной безопасности / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : ИЦ "Академия", 2009. - 272с. - 18 экз.
3. Варфоломеев, А.А. Основы информационной безопасности [Электронный ресурс] / А. А. Варфоломеев. - Приоритетн. нац. проект "Образование", РУДН. - 2 Мб. - Москва : РУДН, 2008. - 1 файл. - Систем. требования: Acrobat Reader

Дополнительная:

1. Мельников, В.П. Информационная безопасность и защита информации / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - М. : ИЦ "Академия", 2009. - 336с. - 2 экз.
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] / В. Ф. Шаньгин. - 74 Мб. - 2012. - 1 файл. - Систем. требования: Acrobat Reader.

Учебно-методические издания, разработанные в ДонНТУ:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине "Управление информационной безопасностью" = Методичні рекомендації для самостійної роботи студентів з навчальної дисципліни "Управління інформаційною безпекою" [Электронный ресурс] : галузь знань: 1701 Інформаційна безпека : напрям підготовки: 6.170102 Системи технічного захисту інформації / Державний вищий навчальний заклад "Донецький національний технічний університет", Факультет радіотехніки і спеціальної підготовки ; ДВНЗ "ДонНТУ", Фак. радіотехніки і спец. підготовки, Каф. радіотехніки та захисту інформації ; уклад. І.Л. Щербов. - 6 Мб. - Донецьк : ДВНЗ "ДонНТУ", 2013. - 1 файл. - Систем. вимоги: Acrobat Reader.

Периодические издания:

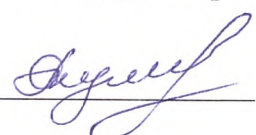
1. Вестник Иркутского государственного технического университета (2014 - 2015).
2. «Бизнес и безопасность» (2014).
3. Экономическая безопасность в бизнесе (2014).
4. Деньги и кредит (208-2013)

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. **Лекционные занятия:** проводятся в аудиториях учебных корпусов согласно расписанию. Аудитория должна соответствовать стандартным требованиям, предъявляемым к лекционным аудиториям. К оснащению лекционных аудиторий дополнительные требования не предъявляются.
2. **Лабораторные занятия:** специализированная лаборатория по инженерно-технической защите информации:
 - генератор шума "Базальт-5 ГЭШ";
 - генератор шума "Базальт-2 ГС" ;
 - генератор шума "Марс ТЗО-4-2";
 - комплекс измерительный FSM-11;

- комплекс измерительный FSM-8.5;
- селективный нановольтметр U-233;
- имитатор сигналов Шиповник-2;
- поисков. устр. мини-в/камер RAY(ЛУЧ);
- разделительный трансформатор 1,5кВт;
- раб. станция в защ. исп. ЗОТ ПЛАЗМА-3В-РС;
- комплекс поиска закл. устр-в ТИКОС-19;
- криптографич. экран "Славутич";
- измер. комплекс FSM-11;
- измер. комплекс FSM-8.5;
- комплекс измер.-вычисл. "Ореол-2";
- АРМ в защ. исполн. ЗОТ "Плазма-3В-АРМ";
- нелинейный локатор NR-M;
- программно-аппарат. комплекс КВАДРАТ;
- видеокамера вариф. Provision PV-717HR;
- видеокамера варифокальная CCTV DG-415;
- виброизлуч. на сист. отопления ВИ-4;
- виброизлучатель ВИ-3;
- генер. шума для защиты моб. тел. ГШМ-02;
- уст. защ. инф. в аналоговых аб. линиях;
- уст. защиты инф. в цифр. абон. линиях;
- уст. защиты на сигн. "Рикас-8С;
- парты;
- доска;
- стол приставной;
- стул полумягкий.

По выполненным лабораторным работам студент составляет отчеты. Отчёт оформляется на листах формата А4 в соответствии с требованиями, предъявляемыми кафедрой Радиотехники и защиты информации к отчётам о лабораторных работах. Защита отчетов происходит публично на аудиторном занятии преподавателю, ведущему занятия.

Составитель рабочей программы:  Якушина А.Е.