2014

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор по УМР
_____ А.А.Панфилов
«_07_» _____04_____ 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы защиты информации

Направление подготовки11.03.02 «Инфокоммуникационные технологии в системах»

Профиль /программа подготовки-

Уровень высшего образования: бакалавриат

Форма обучения: очная

Семестр	Трудоем-кость зач. ед,час.	Лек-ций, час.	Практич. занятий, час.	Лабор. занятий, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
4	2/72	18		18	36	зачет
Итого	2/72	18		18	36	зачет

Владимир, 2015

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина читается в 4 семестре и является одной из важнейших, завершающих дисциплин в подготовке бакалавра по специальности11.03.02.

Целями освоения дисциплины являются:

- получение представления о современном несанкционированном доступе к информации и защите от него;
- выработка у студентов основных навыков в информационной защите предприятий и физических лиц от несанкционированного доступа;
- ознакомление студентов с основными видами несанкционированного доступа к конфиденциальной информации;
- знакомство с аппаратурными и программными методами борьбы с несанкционированным доступом;
- подготовка для разных сфер профессиональной деятельности специалиста:
  - научно-исследовательской.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Базовая часть. Код основной образовательной программы (раздела) – Б1.В.ДВ4.1.

Взаимосвязь с другими дисциплинами

Курс основывается на знании математики, теории информации, других радиотехнических дисциплин и является базой для подготовки выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен обладать следующими

Общекультурными компетенциями (ОК):

- способен находить организационно-управленческие решения в нестандартных ситуациях и готов нести за них ответственность (ОК-4);

профессиональными компетенциями (ПК):

- готовностью учитывать современные тенденции развития электроники, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности (ПК-3);
- способен владеть методами решения задач анализа и расчета характеристик радиотехнических цепей (ПК-1);
- способен собирать, обрабатывать, анализировать и систематизировать научно-

техническую информацию по тематике исследования, использовать достижения отечественной и зарубежной науки, техники и технологии (ПК-2).

В результате освоения дисциплины обучающийся должен:

Знать:

- основы защиты информации;
- современные тенденции развития телекоммуникационной техники;
- основы организации защиты от несанкционированного доступа.

Уметь:

- использовать основные приемы обработки экспериментальных данных;
- применять действующие стандарты, положения и инструкции по оформлению технической документации;
- выполнять задания в области защиты информации предприятий.

Владеть:

- методологией исследований и основными приемами обработки данных;
- методологией построения структур защищенных информационных систем в условиях производства и эксплуатации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа). Распределение трудоемкости по видам занятий представлено в табл. 1.

Таблица 1

№ п/п	Раздел дисциплины	семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы с применением Интерактивных методов (в часах/%)	Формы текущего контроля успеваемости *(по неделям)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП/КР		
1	Введение определения. Конкуренция. Промышленный шпионаж. Объекты конфиденциальных интересов. Документы. Телефоны, ЭВМ и т.п.	4	1.	2				2		1/50	
			2.			2		2		0,5/25	
			3.	2				2		1/50	
			4.			2		2		0,5/25	
			5.	2				2		0,5/25	
2	Подслушивание. Наблюдение. Хищение. Копирование. Подделка. Уничтожение. Незаконное подключение. Перехват. Фотографирование. Сбор и аналитическая обработка. Цели и задачи системы безопасности. Объекты защиты. Основные виды угроз интересам предприятия. Управление безопасностью.					2		2		1/50	Рейтинг контроль №1
			6.	2				2		1/50	
3	Правовая защита. организационная защита. Инженерно-техническая защита. Аппаратные		7.			2		2		1/50	
			8.	2				2		1/50	
			9.			2		2		0,5/25	

	средства. Программные средства защиты информации. Математические и криптографические средства. Личные меры безопасности (технические средства). Безопасность на рабочем месте. Безопасность квартиры. Обеспечение безопасности предпринимателя и членов его семьи.		10.	2				2		1/50	Рейтинг контроль №2
			11.			2		2		1/50	
			12.	2				2		0,5/25	
4	Организационные меры защиты. Аппаратные средства. Программные средства. Криптографические средства защиты.		13.			2		2		1/50	
			14.	2				2		0,5/25	
			15.			2		2		1/50	
			16.	2				2		1/50	
			17.			2		2		1/50	Рейтинг контроль №3
Всего часов		72		18		18		36		15/42	зачет

5.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

5.1. Активные и интерактивные формы обучения

С целью формирования и развития профессиональных навыков студентов в учебном процессе используются активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой: (индивидуальные домашние контрольные работы и доклады по ним, темы приведены далее, п.6.1)).

5.2. Самостоятельная работа студентов

Самостоятельная (внеаудиторная) работа студентов включает закрепление теоретического материала при подготовке к выполнению и защите практических заданий, а также при выполнении индивидуальной домашней работы. Основа самостоятельной работы - изучение литературы по рекомендованным источникам и конспекту лекций. (Вопросы

приведены далее, п.6.2).

5.3. Мультимедийные технологии обучения

Лекционные занятия проводятся частично в виде презентаций в мультимедийной аудитории с использованием компьютерного проектора и представлением от 5 до 40 слайдов по каждой лекции.

Студентам предоставляется компьютерный курс лекций. Компьютерные технологии используются для оформления самостоятельных работ.

5.4.Рейтинговая система обучения

Рейтинг-контроль проводится 3 раза за семестр. Он предполагает оценку суммарных баллов по следующим составляющим: активность на контрольных занятиях; качество выполнения домашних заданий и самостоятельных работ.

(Вопросы приведены далее, п.6.3).

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контрольная работа выполняется по индивидуальному заданию в рамках внеаудиторных занятий. Работа посвящена отчету по проекту защиты от несанкционированного доступа какого-либо предприятия.

Текстовая, расчетная и графическая часть работы оформляется в виде пояснительной записки в соответствии с действующими стандартами России и ВлГУ. Работа может быть проведена и оформлена по современным информационным технологиям.

6.1. ТЕМЫ КОНТРОЛЬНЫХ РАБОТ

1.Виды информации на предприятиях.

2.Основные объекты защиты информации.

3.Технический канал утечки информации.

4.Физическая природа различных каналов.

5.Защита речевой информации.

6.Устранения несанкционированного использования диктофонов.

7.Защита телефонных линий

8. Устройства перехвата информации

9. Поиска устройств перехвата информации.

10. Выявления радиозакладок.

11. Защита технических каналов связи.

12. Влияние проникновений на эффективность каналов связи.

6.2. Вопросы к СРС

1. Какие виды информации существуют на предприятиях?
2. Что такое технический канал утечки информации?
3. Физическая природа различных каналов.
4. Особенности защиты речевой информации.
5. Возможные пути устранения несанкционированного использования диктофонов.
6. Основные методы защиты телефонных линий.
7. Основные характеристики устройств перехвата информации
8. Основные методы поиска устройств перехвата информации.
9. Основные методики проверки учреждений и предприятий.
10. Основные экономические подходы при оценке целесообразности защиты технических каналов связи.

11. Главные потери при перехвате информации.
12. Влияние проникновений на эффективность каналов связи.

6.3.Список вопросов к рейтинг-контролю

Контрольные вопросы к рейтинг-контролю 1

1. Какие виды информации существуют на предприятиях?
2. Укажите основные объекты защиты информации.
3. Укажите разницу между сосредоточенной и распределенной антеннами.
4. Что такое технический канал утечки информации?
5. Физическая природа различных каналов.
6. Особенности защиты речевой информации.
7. Возможные пути устранения несанкционированного использования диктофонов.
8. Основные методы защиты телефонных линий.

Контрольные вопросы к рейтинг-контролю 2

1. Основные характеристики устройств перехвата информации
2. Основные методы поиска устройств перехвата информации.
3. Основные отличия между сканером и интесептором.
4. Основные методики проверки учреждений и предприятий.
5. Пути выявления радиозакладок.
6. Профилактические мероприятия для учреждений и предприятий по защите технических каналов связи.

Контрольные вопросы к рейтинг-контролю 3

1. Основные экономические подходы при оценке целесообразности защиты технических каналов связи.
2. Возможные критерии оценок.
3. Главные потери при перехвате информации.
4. Выигрыш при защите информации в технических каналах связи учреждений и предприятий.
5. Влияние проникновений на эффективность каналов связи.
6. Необходимость выявления проникновений в информационные каналы связи.

6.4. Вопросы к зачету

1. Какие виды информации существуют на предприятиях?
2. Укажите основные объекты защиты информации.
3. Укажите разницу между сосредоточенной и распределенной антеннами.

4. Что такое технический канал утечки информации?
5. Физическая природа различных каналов.
6. Особенности защиты речевой информации.
7. Возможные пути устранения несанкционированного использования диктофонов.
8. Основные методы защиты телефонных линий.
9. Основные характеристики устройств перехвата информации
10. Основные методы поиска устройств перехвата информации.
11. Основные отличия между сканером и интесептором.
12. Основные методики проверки учреждений и предприятий.
13. Пути выявления радиозакладок.
14. Профилактические мероприятия для учреждений и предприятий по защите технических каналов связи.
15. Основные экономические подходы при оценке целесообразности защиты технических каналов связи.
16. Возможные критерии оценок.
17. Главные потери при перехвате информации.
18. Выигрыш при защите информации в технических каналах связи учреждений и предприятий.
19. Влияние проникновений на эффективность каналов связи.
20. Необходимость выявления проникновений в информационные каналы связи.

7.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Литература

1.Информационная безопасность и защита информации[Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - http://www.studentlibrary.ru/book/ISBN9785940747680.html

2.Защита информации от несанкционированного доступа: метод.указания к выполнению лабораторной работы по курсу "Аттестация объектов информатизации" [Электронный ресурс] / А.А. Герасимов, А.В. Мозговой. - М. : Издательство МГТУ им. Н. Э. Баумана, 2012." - http://www.studentlibrary.ru/book/bauman_0485.html

3.Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html

Дополнительная литература

1.Радиолокация. Радионавигация. Радиоуправление. Телевизионная техника. : реферативный журнал (РЖ) : электронное издание .— Москва : Всероссийский институт научной и технической информации (ВИНИТИ), №№ 1-12,- 2010, 2011, 2012 гг.

2.Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN9785940745181.html

3.Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN9785940745181.html

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает:

- кафедральные мультимедийные средства (ауд. 311-3);
- наборы слайдов по всем лекциям (от 25 до 40 слайдов по каждой лекции) и учебные фильмы;
- компьютеры со специализированным программным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению «Инфокоммуникационные технологии в системах»

Рабочую программу составил профессор кафедры РТ и РС, д.т.н.- А.П. Галкин

Сторонний рецензент _____ ген. директор «ВКБР», к.т.н.А.Е. Богданов

Программа рассмотрена и одобрена на заседании кафедры
протокол № 13 от 6.04.15 года.
Заведующий кафедрой РТ и РС О.Р. Никитин

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления «Инфокоммуникационные технологии в системах»

протокол № 10 от 7.04.15

Председатель комиссии О.Р. Никитин

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Программа переутверждена:

на 16/17 учебный год, протокол № 1 от 1.09.16

Зав. кафедрой _____ ОР Ниязбан

на_____учебный год, протокол №_____от _____

Зав. кафедрой _____

на_____учебный год, протокол №_____от _____

Зав. кафедрой _____

на_____учебный год, протокол №_____от _____

Зав. кафедрой _____

на_____учебный год, протокол №_____от _____

Зав. кафедрой _____