МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

А.М. Голиков

ЗАЩИТА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Учебно-методические указания для самостоятельной работы студентов

Томск, 2015

Голиков А.М. Защита информации в инфокоммуникационных системах и сетях: Учебно-методические указания для самостоятельной работы студентов**. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 10 с.**

Учебно-методические указания для самостоятельной работы студентов содержат методические указания для самостоятельной работы студентов (СРС) по подготовке к практическим занятиям, выполнению индивидуальных заданий и вопросы для подготовки к экзамену, а также организации труда студентов при подготовке курса «Защита информации в инфокоммуникационных системах и сетях», являющийся курсом, который включен в Государственный образовательный стандарт по специальности - 210601.65 - Радиоэлектронные системы и комплексы (**с**пециализация - 210601-2.65 - Радиоэлектронные системы передачи информации).

1. Цели и задачи дисциплины:

Дисциплина "Защита информации в инфокоммуникационных системах и сетях" (ЗИвИКСиС) относится к числу дисциплин специализации С3+В1.1 рабочего учебного плана для подготовки инженеров по специальности 210601.65-Радиоэлектронные системы и комплексы (специализация 210601-2.65 Радиоэлектронные системы передачи информации). Целью преподавания дисциплины является изучение методов защиты и основных закономерностей передачи информации в цифровых телекоммуникационных системах.

Основной задачей дисциплины является формирование у студентов *компетенций*, позволяющих самостоятельно проводить математический анализ физических процессов в аналоговых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчивости телекоммуникационных систем и сетей.

В курсе ЗИвИКСиС принят единый методологический подход к анализу и синтезу современных телекоммуникационных систем и устройств на основе вероятностных моделей сообщений, сигналов, помех и каналов в системах связи. Предусмотренные программой курса ЗИвИКСиС знания являются не только базой для последующего изучения специальных дисциплин, но имеют также самостоятельное значение для формирования инженеров по специальности 210601.65 Радиоэлектронные системы и комплексы.

2. Место дисциплины в структуре ООП

Дисциплина ЗИвИКСиС относится к числу специальных дисциплин С3+В1.5 рабочего учебного плана подготовки инженеров.

Теоретической базой курса ЗИвИКСиС *являются основные сведения из дисциплин естественнонаучного и профессионального циклов подготовки инженеров: Теория вероятности и статистика в радиоэлектронике, Информационные технологии, Основы теории радиосистем передачи информации.*

Минимальным требованием к «входным» знаниям, необходимым для успешного усвоении данной дисциплины, является удовлетворительное усвоение программ по указанных выше курсам.

Изучаемая дисциплина является предшествующей при изучении специальных и профилирующих дисциплин: Кодирование и шифрование информации в системах связи, Системы радиосвязи, Инженерно-техническая защита информации, а также может быть использована при подготовке выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины:

Изучение рассматриваемой дисциплины направлено на формирование у студентов следующих **компетенций:**

способностью разрабатывать структурные и функциональные схемы мобильных, широкополосных и спутниковых систем передачи информации (ПСК-2.1);

способностью оценивать основные показатели качества систем передачи информации с учетом характеристик каналов связи (ПСК-2.2);

способностью проводить оптимизацию радиосистем передачи информации и отдельных её подсистем (ПСК-2.3);

способностью проводить компьютерное проектирование и моделирование радиоэлектронных систем передачи информации и их подсистем (ПСК-2.4).

В результате изучения дисциплины студент должен:

знать

- роль и место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства;
- современные подходы к построению систем защиты информации;
- компьютерные системы и сети как объект информационного воздействия, критерии оценки их

защищенности и методы обеспечения их информационной безопасности

уметь

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;

- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;

- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований;

владеть

- анализом информационной инфраструктуры государства;

- методами формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей.

Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Вид учебной работы	Всего часов	Семестры	
		9	
Аудиторные занятия (всего)	72	72	
В том числе:	- -		
Лекции	36	36	
Лабораторные работы (ЛР)	18	18	
Практические занятия (ПЗ)	18	18	
Курсовая работа (КР)	нет	нет	
Самостоятельная работа (всего)	36	36	
Вид промежуточной аттестации – экзамен 7 сем.	36	36	
Общая трудоемкость час	144	144	
Зачетные Единицы Трудоемкости	4	4	

Содержание дисциплины

Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час.	Лаборат. занятия, час.	Практич. Занятия, час.	Курсовой П/Р (КСР)	СРС час. (без экзам.)	Всего, час. (без экзам.)	Формируемые компетенции (ОК, ПК)
1.	Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	2	-	-	-	2	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
2.	Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.	6	4	4	-	6	20	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
3.	Методы и средства обеспечения	6	8	6	-	4	24	ПСК-2.1, ПСК-2.2,

	информационной безопасности.							ПСК-2.3, ПСК-2.4
4.	Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности.	10	4	4	-	10	28	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
5.	Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей	8	4	4	-	8	24	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
6.	Методология построения и анализа систем обеспечения информационной безопасности.	4			-	6	10	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
	Всего	36	18	18	-	36	108	

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и сопутствующими дисциплинами

№ п/п	Наименование обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины из табл.5.1, для которых необходимо изучение обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин								
		1	2	3	4	5				
Предшествующие дисциплины										
1	Теория вероятности и статистика в радиоэлектронике		+	+						
2	Информационные технологии	+	+	+						
3	Основы теории радиосистем передачи информации	+	+	+	+	+				
Последующие дисциплины										
1	Кодирование и шифрование информации в системах связи	+	+	+	+	+				

2	Системы радиосвязи		+	+	+	+				
3	Инженерно-техническая защита информации		+	+	+	+				

Лабораторный практикум

№ п/п	№ Раздела дис-циплины из табл. 5.1	Тематика лабораторных занятий	Трудо-емкость (час.)	Компетенции ОК, ПК
1	5	Изучение международного стандарта безопасности информационных систем ISO 17799	2	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
2	5	Система анализа рисков и проверки политики информационной безопасности предприятия	4	
3	3	Исследование системы защиты информации «Страж NT»	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
4	3	Система защиты информации SecretNet	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
5	6	Система защиты информации Dallas	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4

Практические занятия

№ п/п	№ Раздела дис-циплины из табл. 5.1	Тематика практических занятий (семинаров)	Трудо-емкость (час.)	Компетенции ОК, ПК
1	2	Стандарты информационной безопасности и критерии оценки безопасности компьютерных систем и сетей	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
2	3	Разработка архитектуры модели безопасности информационных систем и сетей	6	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
3	4	Разработка практических рекомендаций по обеспечению безопасности информационных систем	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4
5	5	Законодательство в области информационной безопасности	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4

Самостоятельная работа (36 час.)

№ п/ п	№ Раздела дисципли-ны из табл. 5.1	Тематика самостоятельной работы (детализация)	Трудо-емкость (час.)	Компетенции ОК, ПК	Контроль вы-полнения рабо-ты
1	1	Криптографические методы и средства защиты информации в компьютерных системах и сетях	2	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4	Выполнение домашнего ин-дивидуальног о задания
2	2	Политика и модели безопасности	6	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4	Контрольная работа.
3	3	Безопасность сетевых операционных систем	4	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4	Выполнение домашнего ин-дивидуальног о задания
4	4	Безопасность локальных и глобальных сетевых технологий	10	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4	Выполнение домашнего ин-дивидуальног о задания
5	5	Радиоэлектронные системы и устройства защиты информации	8	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4	Выполнение домашнего ин-дивидуальног о задания
6	6	Комплексная защита информации в компьютерных системах и сетях	6	ПСК-2.1, ПСК-2.2, ПСК-2.3, ПСК-2.4	Выполнение домашнего ин-дивидуальног о задания

СРС включает в себя подготовку к лекциям, практическим занятиям и лабораторным работам, а также подготовке индивидуальной работы в форме реферата. Перечень тем рефератов приведен ниже.

ПЕРЕЧЕНЬ
индивидуальных заданий по курсу «Защита информации в инфокоммуникационных системах и сетях»

№ п/п	Тема
1.	Система защиты информации "SecretNet"
2.	Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet Custom
3.	Система защиты информации от несанкционированного доступа "Страж"
4.	*Исследование защищенной системы хранения данных на базе программного обеспечения с открытым исходным кодом*
5.	Система защиты информации "SecretNet"
6.	Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ
7.	Система защиты информации Dallas Lock
8.	Защита беспроводных сетей стандартов IEEE 802.11
9.	*Исследование методов аналогового скремблирования на базе LabView*
10.	Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet CSP

11.	Защита беспроводных сетей стандартов IEEE 802.15
12.	*Исследование защищенной многоточечной видеоконференц связи на базе WEB-технологии*
13.	Защита беспроводных сетей стандартов GSM, CDMA
14.	Защита беспроводных сетей стандартов WiMAX
15.	Защита беспроводных сетей стандартов LTE
16.	Исследование технологии множественного доступа на базе OFDM-модуляции и технологии MIMO
17.	Формальные политики и математические модели компьютерной безопасности
18.	Организация защиты сетей CISCO
19.	Обзор и анализ наиболее важных стандартов и спецификаций в области информационной безопасности
20.	Обзор и анализ классических криптографических шифров
21.	Обзор и анализ симметричных криптографических шифров
22.	Обзор и анализ ассиметричных криптографических шифров
23.	Программные комплексы для создания криптовалюты Биткойн
24.	Алгоритм шифрования данных AES и его программная реализация
25.	Инфраструктуры открытых ключей PKI

Кроме времени, выделенного на СРС, согласно учебного плана студентам выделено время для подготовки к экзамену (36 часов). До экзамены студентам выдаются вопросы для подготовки.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.
19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
22. Классификация требований к средствам защиты информации.
23. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
24. Требования к защите, обусловливаемые видом защищаемой информации.
25. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
26. Анализ существующих методик определения требований к защите информации.

27. Стандарт США «Критерии оценки гарантировано защищенный вычислительных систем в интересах Министерства обороны США». Основные положения.
28. О Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. 1.
29. Классы защищенности средств вычислительной техники от несанкционированного доступа.
30. Факторы, влияющие на требуемый уровень защиты информации.
31. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты.
32. Методы формирования функций защиты.
33. События, возникающие при формировании функций защиты.
34. Классы задач функций защиты.
35. Класс задач функций защиты 1 - уменьшение степени распознавания объектов.
36. Класс задач функций защиты 2 - защита содержания обрабатываемой, хранимой и передаваемой информации.
37. Класс задач функций защиты 3 - защита информации от информационного воздействия.
38. Функции защиты информации.
39. Стратегии защиты информации.
40. Способы и средства защиты информации.
41. Способы «абсолютной системы защиты».
42. Архитектура систем защиты информации. Требования.
43. Общеметодологических принципов архитектуры системы защиты информации.
44. Построение средств защиты информации.
45. Ядро системы защиты информации.
46. Семирубежная модель защиты.

Учебно-методическое и информационное обеспечение дисциплины:
Основная литература

1. Акулиничев Ю. П., Бернгардт А. С. Теория и техника передачи информации: Учебное пособие. -Томск: Томск. гос. ун-т систем управления и радиоэлектроники,2011. - 190с. Режим доступа: http://edu.tusur.ru/training/publications/1750

2. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ / Голиков А. М. – 2012. 374 с.// https://edu.tusur.ru/training/publications/1050

3. Голиков А.М. Методы шифрования информации в сетях и системах радиосвязи: Сборник лабораторных работ. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2012. – 333 с. Режим доступа: http://edu.tusur.ru/training/publications/1051

4. Системы радиосвязи: Сборник лабораторных работ / Голиков А. М. – 2012. 169 с.// https://edu.tusur.ru/training/publications/1052

Дополнительная литература

1. Акулиничев Ю.П. Теория электрической связи: учеб. пособие. - Томск:, ТУСУР, 2007. - 214 с. (100 экз.)

2. Голиков А.М. Транспортные и мультисервисные системы и сети связи: 2012. – 292 с.: Сборник лабораторных работ. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2012. – 292 с. Режим доступа: http://edu.tusur.ru/training/publications/1111

Программное обеспечение

1. Операционная система Windows.
2. Matlab, LabView.
3. Информационно-справочные и поисковые системы.

Материально-техническое обеспечение дисциплины:

1. Учебно-методический комплекс дисциплины:

- Ю.П. Акулиничев, А.С. Бернгардт. Теория и техника передачи информации: Учебное пособие. -Томск: 2011. -190с. Режим доступа: http://edu.tusur.ru/training/publications/1750

- **Голиков А.М.** Транспортные и мультисервисные системы и сети связи: 2012. – 292 с.: Сборник лабораторных работ. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2012. – 292 с. Режим доступа: http://edu.tusur.ru/training/publications/1111

- Теория и техника передачи информации: Учебно-методическое пособие для проведения практических занятий и самостоятельной работы студентов / Акулиничев Ю. П. - 2012. 202 с. Режим доступа: http://edu.tusur.ru/training/publications/1754

- Тестовые вопросы для самоконтроля.

-Оборудование лаборатории информационной безопасности телекоммуникационных систем

- ауд. 401 радиотехнического корпуса.

2. Персональные компьютеры с доступом в сеть Интернет.

3. Демонстрационный телевизор.

4. Фломастерная доска.

13. Методические рекомендации по организации изучения дисциплины

Основная рекомендация сводится к обеспечению равномерной активной работы студентов над курсом в течение учебного семестра.

При изучении курса следует стараться понять то общее, что объединяет рассматриваемые вопросы. Например, для методов *передачи* сигналов ключевым является понятие *избыточности и ее роль при передаче информации.* Для методов *приема* общей является идея *уменьшения апостериорной неопределенности* относительно передаваемого сигнала по сравнению с априорной неопределенностью.