

ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.11.ДВ.01.02 Информационная безопасность в радиотехнических системах

(Шифр и полное название дисциплины в соответствии с учебным планом)

Направление подготовки: 11.03.01 Радиотехника, 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Радиоинформатика, мониторинг и телеметрия

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: физики, радиотехники и электроники

	очная форма	очно-заочная форма	заочная форма
Курс	4	-	-
Семестр/триместр	8	-	-

Лекции	44	-	-
Лабораторные занятия	22	-	-
Практические (семинарские) занятия	22	-	-
Консультации		-	-
Форма(ы) промежуточной аттестации	зачет	-	-
Контроль	-	-	-
Иные формы работы	-	-	-
Самостоятельная работа	56	-	-

Всего часов: 144

Трудоемкость: 4 зачетных единицы.

Разработчик рабочей программы:

ст. преподаватель _____ Арнаутов Е.А.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: является формирование у студентов устойчивых основ знаний организации информационной безопасности радиотехнических систем, приобретения при этом необходимых умений и навыков.

Задачи изучения дисциплины:

- изучение сущности и задач системы защиты информации (СЗИ) в радиотехнических системах (РТС);
 - изучение принципов организации и этапов разработки СЗИ РТС, факторов, влияющих на организацию СЗИ РТС;
 - определение и нормативное закрепление состава защищаемой информации; определение объектов защиты;
 - анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию;
 - определение потенциальных каналов и методов несанкционированного доступа к информации, определение возможностей несанкционированного доступа к защищаемой информации;

Место дисциплины в структуре ОПОП:

Дисциплина Б1.В.01.11.ДВ.01.02 «Информационная безопасность в радиотехнических системах» реализуется в рамках Модуля 5 «Радиоинформатика, мониторинг и телеметрия» части ОПОП, формируемой участниками образовательных отношений.

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-1 Способен осуществлять поиск, критический анализ и синтез информации и применять системный подход для решения поставленных задач	Знать: <ul style="list-style-type: none">- методы поиска информации и работы с ней;- сущность системного подхода;	Знает: <ul style="list-style-type: none">- основы организации и управления системой защиты информации в радиотехнических системах
	Уметь: <ul style="list-style-type: none">- анализировать задачу, выделять этапы ее решения, осуществлять действия по решению;- находить различные варианты решения задачи, оценивать их преимущества и риски;	Умеет: <ul style="list-style-type: none">- выбирать и разрабатывать оптимальный алгоритм для его дальнейшей реализации при решении задач защиты информации;- осуществлять оптимизацию примененного решения.
	Владеть: <ul style="list-style-type: none">- навыками оценивания практических последствий возможных вариантов решения задачи;- навыками грамотного, логичного,	Владеет: <ul style="list-style-type: none">- методикой тестирования радиотехнических систем;- способами реализации защиты информации.

	аргументированного формулирования собственных суждений и оценок	
ПКС-1 Способен производить расчеты, необходимые для проектирования и эксплуатации оборудования систем связи и линий связи	Знать: - правила технической эксплуатации систем связи и линий связи; - основные этапы проектирования систем связи и линий связи	Знает: - кадровое, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ РТС; – назначение, структуру и содержание управления СЗИ РТС
	Уметь: - производить расчет систем связи и линий связи	Умеет: - разрабатывать организационные и технические мероприятия по защите информации;
	Владеть: - специализированными методиками расчета, навыками чтения и формирования технического задания, средствами автоматизированного проектирования	Владеет: - навыками внедрения систем защиты информации в радиотехнических системах;

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№ п/п	Наименование разделов и тем	Всего	Аудиторные занятия			Сам. раб.
			ЛК	ПЗ	ЛБ	
8 семестр						
	Раздел 1. Введение					
1	Тема 1. Система защиты информации в радиотехнических системах	6	2			4
2	Тема 2. Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации .	6	2			4
	Раздел 2. Определение компонентов СЗИ РТС					
3	Тема 3. Каналы утечки информации - оптический, акустический, радиоэлектронный	24	6	6	6	6
4	Тема 4. Методы защиты от	6	2			4

	несанкционированного перехвата речевой, визуальной, оптической, радио- электронной информации					
5	Тема 5. Радиомониторинг	16	4	2	6	4
6	Тема 6. Криптографическая защита информации	16	6	6		4
7	Тема 7. Физическая защита информации	14	6	4		4
8	Тема 8. Принципы, силы, средства и условия организационной защиты информации	6	2			4
9	Тема 9. Определение сил и средств, необходимых для защиты информации.	6	2			4
	Раздел 3. Построение системы защиты информации					
10	Тема 10. Разработка моделей систем защиты информации телекоммуникационных систем	18	4	2	6	6
11	Тема 11. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации	8	2	2		4
12	Тема 12. Нормативно-методическое обеспечение функционирования СЗИ РТС	6	2			4
13	Тема 13. Архитектурное построение системы защиты информации	12	4		4	4
	Контроль:					
	Форма отчетности: зачет					
	Итого за 8 семестр	144	44	22	22	56
	ИТОГО:	144	44	22	22	56

Очно-заочная форма обучения не реализуется

Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме выполнения контрольной работы

Типовые варианты контрольной работы

1. Как определяется системный подход и его понятие.
2. Дать понятие системы обеспечения информационной безопасности организации.

1. Система защиты информации организации, понятие и взаимосвязь с другими разделами дисциплины.
2. Защищаемая информация, определение и понятие.

1. Организация защиты информации на предприятии, существо и методика.
2. Техника защиты информации. Определение, понятие и взаимосвязь с другими разделами дисциплины.

1. Контролируемая зона. Определение, понятие, цели и задачи установления.
2. Технический канал утечки информации (ТКУИ). Понятие и физический смысл.

1. Подсистема технической защиты информации на предприятии. Определение, понятие, состав, роль и место в обеспечении защиты информации.
2. Подсистема организационно-правовой защиты информации на предприятии. Определение, понятие, структура и состав, роль и место в обеспечении защиты информации.

1. Подсистема криптографической защиты информации. Определение, понятие, состав, роль и место в обеспечении защиты информации.
2. Подсистема физической защиты информации на предприятии. Определение, понятие, структура и состав, роль и место в обеспечении защиты информации.

Вопросы к зачету (8 семестр, очная форма обучения)

1. Информационная безопасность РТС. Объект ИРТС. Определение и понятие.
2. Системный подход. Определение и понятие.

3. Модель системы обеспечения информационной безопасности организации. Определение и понятие.
4. Модель системы защиты информации организации. Определение и понятие.
5. Модель объекта защиты информации. Определение и понятие.
6. Модель защищаемой информации. Определение и понятие.
7. Модель защиты информации. Определение и понятие.
8. Модель организации защиты информации. Определение и понятие.
9. Техника защиты информации. Определение и понятие.
10. Модель контроля защиты информации. Цель и понятие.
11. Контролируемая зона. Определение и понятие.
12. Модель технического канала утечки информации (ТКУИ), виды ТКУИ. определение, понятие, физический смысл.
13. Модель подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Понятие.
14. Модель подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Понятие.
15. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.
16. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров.
17. Модель уязвимостей системы обеспечения ИБ организации. Определение и понятие.
18. Модель нарушителя ИБ организации. Определение и понятие.
19. Модель технической реализации ПТЗИ ОИ.
20. Модель нейтрализации угроз БИ на предприятии.
21. Модель подсистемы физической защиты информации объекта информатизации на предприятии.
22. Модель периметральной защиты объекта информатизации на предприятии.
23. Модель защиты информации от несанкционированного доступа (НСД). Определение и понятие.
24. Основа концепции защиты СВТ и АС от НСД к информации.
25. Классификация АС. Цели и основные понятия.
26. Аттестация объектов информатизации. Понятие.
27. Модель приобретения ПЭВМ в защищенном исполнении.
28. Доктрина ИБ РФ. Общие положения.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576726> 1 (дата обращения: 01.04.2024). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

4.2. Дополнительная литература

2. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие : / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёткин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=5986651>. (дата обращения: 01.04.2024). – Библиогр.: с. 116 - 120. – ISBN 978-5-9275-3431-9. – Текст : электронный.

3. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> 1. (дата обращения: 01.04.2024). – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	https://ru.cppreference.com/w/	Он-лайн справочник по языку C/C++	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ

И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1	http://window.edu.ru	Единое окно доступа к образовательным ресурсам	Свободный доступ
2	https://elibrary.ru	Научная электронная библиотека eLIBRARY.RU	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

- Microsoft Windows XP Professional; Microsoft Windows 7 Professional. Академические лицензии OLP (Open License). Срок действия лицензии: бессрочно.;
- Microsoft Office Professional Plus 2007 (пакет офисных приложений). Академические лицензии OLP (Open License). Срок действия лицензии: бессрочно.
- Code::Blocks IDE – свободно распространяемое ПО.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия проводятся в компьютерном классе.

Оборудование компьютерного класса:

- Персональный компьютер преподавателя (1 шт.)
- Персональный компьютер обучающегося (10 шт.)
- Принтер Samsung ML-1750
- Сканер HP ScanJet 3670
- Сетевое оборудование: коммутатор D-link DGS1016G

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.