

ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.08 Защита информации от утечки по техническим каналам

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	3, 4		
Семестр	6, 7		

Лекции	28		
Лабораторные занятия	56		
Практические (семинарские) занятия	28		
в т. ч. практическая подготовка	4		
Форма(ы) промежуточной аттестации	Экзамен – 0.3 Экзамен – 0.3		
Контроль	18		
Иные формы работы			
Самостоятельная работа	157.4		

Всего часов: 288

Трудоемкость: 8 зачетных единиц.

Разработчик(и) рабочей программы:

кандидат педагогических наук, доцент

Д.А. Таров

І. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование у студентов практических навыков организации и проведения мероприятий по выявлению возможных технических каналов утечки информации на объектах информатизации и в выделенных помещениях и построения системы технической защиты.

Задачи изучения дисциплины:

- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты информации от наблюдения;
- изучение способов и средств защиты конфиденциальной информации от перехвата;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- изучение методов и средств оценки защищенности выделенных (защищаемых) помещений и соответствия их нормативным документам;
- обучение основам построения системы технической защиты информации на объектах информатизации и в выделенных помещениях.

Место дисциплины в структуре ОПОП: реализуется в обязательной части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-9	Знать: – особенности технических и криптографических средств защиты информации, механизмы функционирования основных технических и криптографических средств защиты, характеристики криптографических протоколов.	Знает: – способы перехвата информации в каналах утечки и методы ее защиты техническими и криптографическими методами.
	Уметь: – проводить анализ технических и криптографических средств защиты автоматизированных систем, определять виды информации, подверженной внешним и внутренним угрозам, производить правильный выбор параметров средств защиты информации.	Умеет: – проводить анализ и критически оценивать работоспособность средств защиты информации от утечки по техническим каналам, настраивать средства защиты информации от утечки по техническим каналам.
	Владеть: – базовыми навыками использования технических и криптографических средств защиты информации при решении задач профессиональной деятельности.	Владеет: – навыком использования средств технической и криптографической защиты информации от утечки по техническим каналам.
ОПК-10	Знать: – принципы реализации, развития и	Знает: – принципы защиты

	<p>совершенствования систем обеспечения информационной безопасности предприятия в рамках комплексного подхода;</p> <ul style="list-style-type: none"> – структуру политики информационной безопасности; – основные технические методы и принципы управления информационной безопасностью предприятий отрасли. 	<p>информационной системы предприятия от утечки информации по техническим каналам;</p> <ul style="list-style-type: none"> – групповую политику, политику информационной безопасности предприятия; – методы и принципы осуществления политики информационной безопасности предприятия.
	<p>Уметь:</p> <ul style="list-style-type: none"> – определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; – разрабатывать политику информационной безопасности объекта защиты; – применять на практике основные механизмы управления информационной безопасностью на объекте защиты. 	<p>Умеет:</p> <ul style="list-style-type: none"> – разрабатывать комплекс мер по обеспечению информационной безопасности ИС; – разрабатывать политику информационной безопасности объекта защиты; – реализовывать политику информационной безопасности объекта защиты.
	<p>Владеть:</p> <ul style="list-style-type: none"> – навыками планирования и организации системы защиты информации; – навыками реализации элементов политики информационной безопасности; – методами организации и управления деятельностью служб защиты информации на предприятии. 	<p>Владеет:</p> <ul style="list-style-type: none"> – навыками разработки и реализации политики информационной безопасности ИС предприятия.

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

№	Наименование разделов и тем	Всего ча- сов	Аудиторные заня- тия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
6 семестр						
Раздел 1. «Объекты информационной защиты»						
1	Тема 1. Понятие о конфиденциальной информа- ции. Основные свойства информации как предме- та защиты. Виды защищаемой информации. Классификация демаскирующих признаков.	18	2	2	4	10
2	Тема 2. Видовые демаскирующие признаки. Сиг- нальные демаскирующие признаки. Веществен- ные демаскирующие признаки.	18	2	2	4	10
3	Тема 3. Источники и носители информации.	18	2	2	4	10

	Классификация источников и носителей информации. Сущность записи и съема информации с носителя.					
4	Тема 4. Источники сигналов. Источники функциональных сигналов. Побочные электромагнитные излучения и наводки.	18	2	2	4	10
Раздел 2. «Характеристика угроз безопасности информации»						
5	Тема 5. Виды угроз безопасности информации. Органы добывания информации. Принципы ведения разведки. Технология добывания информации.	20	2	2	4	12
6	Тема 6. Способы доступа к конфиденциальной информации. Показатели эффективности разведки. Способы и средства наблюдения. Способы и средства перехвата сигналов. Способы и средства подслушивания.	20	2	2	4	12
Раздел 3. «Способы и средства добывания информации»						
7	Тема 7. Особенности утечки информации. Характеристики технических каналов утечки информации.	18	2	2	4	10
8	Тема 8. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации.	20	2	2	4	12
9	Тема 9. Акустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексирование каналов утечки информации.	20.7	2	2	4	12.7
	<i>Контроль</i>	9				
	<i>Экзамен</i>	0.3				
	Итого за 6 семестр	180	18	18	36	98.7
	в т. ч. практическая подготовка	4		2	2	
<i>7 семестр</i>						
Раздел 4. «Методы инженерной защиты и технической охраны объектов»						
10	Тема 10. Методы защиты информации от утечки по техническим каналам. Защита информации по акустическому каналу. Методы и средства защиты информации от перехвата компьютерной информации.	22	2	2	4	14
Раздел 5. «Организация инженерно-технической защиты информации»						
11	Тема 11. Общие положения по инженерно-технической защите информации в организациях.	22	2	2	4	14
12	Тема 12. Системный подход к защите информации. Моделирование объектов защиты.	22	2	2	4	14
13	Тема 13. Моделирование угроз безопасности информации. Методические рекомендации по разработке мер инженерно-технической защиты информации.	32.7	4	4	8	16.7
	<i>Контроль</i>	9				
	<i>Экзамен</i>	0.3				
	Итого за 7 семестр	108	10	10	20	58.7

	ИТОГО	288	28	28	56	157.4
--	--------------	------------	-----------	-----------	-----------	--------------

Очно-заочная форма обучения не реализуется

Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы.

Типовой вариант контрольной работы

1. Понятие о конфиденциальной информации
2. Основные свойства информации как предмета защиты
3. Виды защищаемой информации
4. Классификация демаскирующих признаков
5. Видовые демаскирующие признаки
6. Сигнальные демаскирующие признаки
7. Вещественные демаскирующие признаки
8. Источники и носители информации
9. Классификация источников и носителей информации
10. Сущность записи и съема информации с носителя
11. Источники сигналов
12. Источники функциональных сигналов
13. Побочные электромагнитные излучения и наводки
14. Виды угроз безопасности информации
15. Органы добывания информации
16. Принципы ведения разведки
17. Технология добывания информации
18. Способы доступа к конфиденциальной информации
19. Добывание информации без физического проникновения в контролируруемую зону
20. Доступ к источникам информации без нарушения государственной границы
21. Показатели эффективности разведки
22. Способы и средства наблюдения
23. Способы и средства наблюдения в оптическом диапазоне
24. Способы и средства наблюдения в радиодиапазоне
25. Способы и средства перехвата сигналов

Промежуточная аттестация обучающихся осуществляется в форме экзамена с использованием следующих оценочных материалов: *перечень вопросов к экзамену.*

Вопросы к экзамену (6 семестр, очная форма обучения)

1. Понятие о конфиденциальной информации. Основные свойства информации как предмета защиты.
2. Виды защищаемой информации. Классификация демаскирующих признаков.
3. Видовые демаскирующие признаки. Сигнальные демаскирующие признаки. Вещественные демаскирующие признаки.
4. Источники и носители информации. Классификация источников и носителей информации.

5. Сущность записи и съема информации с носителя.
6. Источники сигналов. Источники функциональных сигналов. Побочные электромагнитные излучения и наводки.
7. Виды угроз безопасности информации. Органы добывания информации.
8. Принципы ведения разведки. Технология добывания информации.
9. Способы доступа к конфиденциальной информации. Показатели эффективности разведки.
10. Способы и средства наблюдения.
11. Способы и средства перехвата сигналов.
12. Способы и средства подслушивания.
13. Особенности утечки информации. Характеристики технических каналов утечки информации.
14. Оптические каналы утечки информации.
15. Радиоэлектронные каналы утечки информации.
16. Акустические каналы утечки информации.
17. Материально-вещественные каналы утечки информации.
18. Комплексирование каналов утечки информации.

Вопросы к экзамену (7 семестр, очная форма обучения)

1. Методы защиты информации от утечки по техническим каналам.
2. Защита информации по акустическому каналу.
3. Методы и средства защиты информации от перехвата компьютерной информации.
4. Общие положения по инженерно-технической защите информации в организациях.
5. Системный подход к защите информации.
6. Моделирование объектов защиты.
7. Моделирование угроз безопасности информации.
8. Методические рекомендации по разработке мер инженерно-технической защиты информации.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Киренберг, А. Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2023. — 222 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/399665> (дата обращения: 18.04.2024). — Режим доступа: для авториз. пользователей.

4.2. Дополнительная литература

1. Иванов, А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : учебное пособие : / А. В. Иванов. — Новосибирск : Новосибирский государственный технический университет, 2018. — 64 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=575420> (дата обращения: 18.04.2024). — Библиогр. в кн. — ISBN 978-5-7782-3713-1. — Текст : электронный.

2. Иванов, А. В. Оценка защищенности информации от утечки по виброакустическим каналам : учебное пособие : / А. В. Иванов. — Новосибирск : Новосибирский государственный технический университет, 2018. — 76 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=575421> (дата обращения: 18.04.2024). — Библиогр. в кн. — ISBN 978-5-7782-3712-4. — 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://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

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, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

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