ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____/Н.В.Черноусова/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.06 Защита информации от утечки по техническим каналам

Направление подготовки: *10.03.01 Информационная безопасность*
Направленность (профиль): *Организация и технологии защиты информации (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**		
Семестр	**6**		

Лекции	**36**		
Лабораторные занятия	**36**		
Практические (семинарские) занятия	**18**		
в т. ч. практическая подготовка	**4**		
Форма(ы) промежуточной аттестации	**Зачет с оценкой**		
Контроль			
Иные формы работы			
Самостоятельная работа	**54**		

Всего часов: 144
Трудоемкость: 4 зачетных единицы.

Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент С.А. Рощупкин

I. 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 вариативной части (части, формируемой участниками образовательных отношений) блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-6	**Знать:** - свои ресурсы и их пределы (личностные, психофизиологические, ситуативные, временные и т.д.) для успешного выполнения порученной работы.	**Знает:** − способы перехвата информации в каналах утечки; − методы защиты информации от утечки по техническим каналам.
	Уметь: - планировать перспективные цели деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - критически оценивать эффективность использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата.	**Умеет**: − критически оценивать работоспособность средств защиты информации от утечки по техническим каналам.
	Владеть: - навыками реализации намеченной цели деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда;	**Владеет:** − навыком подготовки отчетных материалов по результатам контроля защищенности информации от утечки по техническим каналам.

	- навыками использования предоставляемых возможностей для приобретения новых знаний и навыков.	
ПКС-2	**Знать**: - основные виды и классификацию информационных ресурсов организации (предприятия); - сущность профессиональной деятельности по обеспечению защиты информации в процессе эксплуатации автоматизированных систем.	**Знает:** − методы и методики контроля защищенности информации от утечки по техническим каналам; − средства контроля защищенности информации от утечки по техническим каналам; − отчетные документы, оформляемые по результатам контроля защищенности информации от утечки по техническим каналам;
	Уметь: - выделять из общих информационных ресурсов предприятия информацию, подлежащую защите; - строить модели защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	**Умеет**: − анализировать и оценивать технологический процесс обработки информации, с целью предотвращения ее утечки по техническим каналам; − проводить оценку защищенности информации от утечки по техническим каналам; − оформлять отчетные материалы по результатам контроля защищенности информации от утечки по техническим каналам;
	Владеть: - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем: - навыками реализации моделей защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	**Владеет:** − проведением контроля защищенности информации от утечки по техническим каналам.

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 часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
6 семестр						
Раздел 1. «Объекты информационной защиты»		**40**	**10**	**4**	**10**	**16**
1	Тема 1. Понятие о конфиденциальной информации. Основные свойства информации как предмета защиты. Виды защищаемой информации. Классификация демаскирующих признаков.	9	2	1	2	4
2	Тема 2. Видовые демаскирующие признаки. Сигнальные демаскирующие признаки. Вещественные демаскирующие признаки.	9	2	1	2	4
3	Тема 3. Источники и носители информации. Классификация источников и носителей информации. Сущность записи и съема информации с носителя	12	4	1	3	4
4	Тема 4. Источники сигналов. Источники функциональных сигналов. Побочные электромагнитные излучения и наводки.	10	2	1	3	4
Раздел 2. «Характеристика угроз безопасности информации»		**18**	**4**	**2**	**4**	**8**
5	Тема 5. Виды угроз безопасности информации. Органы добывания информации. Принципы ведения разведки. Технология добывания информации.	9	2	1	2	4
6	Тема 6. Способы доступа к конфиденциальной информации. Показатели эффективности разведки.	9	2	1	2	4
Раздел 3. «Способы и средства добывания информации»		**10**	**2**	**2**	**2**	**4**
7	Тема 7. Способы и средства наблюдения. Способы и средства перехвата сигналов. Способы и средства подслушивания.	10	2	2	2	4
Раздел 4. «Способы и средства добывания информации»		**40**	**12**	**4**	**12**	**12**
8	Тема 8. Особенности утечки информации. Характеристики технических каналов утечки информации.	13	4	1	4	4
9	Тема 9. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации.	13	4	1	4	4
10	Тема 10. Акустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексирование каналов утечки информации	14	4	2	4	4
Раздел 5. «Методы инженерной защиты и технической охраны объектов»		**10**	**2**	**2**	**2**	**4**
11	Тема 11. Методы защиты информации от утечки	10	2	2	2	4

	по техническим каналам. Защита информации по акустическому каналу. Методы и средства защиты информации от перехвата компьютерной информации.					
Раздел 6. «Организация инженерно-технической защиты информации»		**8**	**2**	**2**	**2**	**2**
12	Тема 12. Общие положения по инженерно-технической защите информации в организациях.	8	2	2	2	2
Раздел 7. «Методическое обеспечение инженерно-технической защиты информации»		**18**	**4**	**2**	**4**	**8**
13	Тема 13. Системный подход к защите информации. Моделирование объектов защиты.	9	2	1	2	4
14	Тема 14. Моделирование угроз безопасности информации. Методические рекомендации по разработке мер инженерно-технической защиты информации.	9	2	1	2	4
	Форма отчетности	**Зачет с оценкой**				
	Контроль					
	Итого за 6 семестр	***144***	***36***	***18***	***36***	***54***
	в т.ч. практическая подготовка	***4***		***2***	***2***	
	ИТОГО	**144**	**36**	**18**	**36**	**54**

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 контролируемую 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 зачета с оценкой с использованием следующих оценочных материалов: *перечень вопросов к зачету.*

Вопросы к зачету
(6 семестр, очная форма обучения)

1. Системный подход к защите информации, основные положения. Цели, задачи и ресурсы системы защиты информации. Угрозы безопасности информации и меры по их предотвращению.

2. Понятие о защищаемой информации, виды защищаемой информации. Демаскирующие признаки объектов защиты, их классификация. Видовые демаскирующие признаки, демаскирующие признаки сигналов, демаскирующие признаки веществ.

3. Технические разведки и их цели. Классификация технической разведки по физической природе носителя информации, по видам носителей аппаратуры разведки.

4. Классификация методов инженерной защиты и технической охраны объектов защиты. Подсистема инженерной защиты.

5. Способы и средства обнаружения злоумышленников и пожара. Назначение, задачи. Извещатели, их классификация, принципы работы.

6. Подсистема наблюдения. Подсистема нейтрализации угроз.

7. Основные задачи, структура и характеристика государственной системы защиты информации и противодействия техническим разведкам. Основные руководящие, нормативные и методические документы. Основные организационные и технические меры.

8. Аттестация объектов информатизации, лицензирование деятельности по защите информации, сертификация средств защиты информации.

9. Характеристика объекта информатизации, как объекта защиты от технических разведок. Основные (ОТСС) и вспомогательные (ВТСС) технические средства и системы, их классификация и характеристики. Зоны R2, r1, r1', случайные антенны. Граница контролируемой зоны объекта информатизации. Виды опасных сигналов на ОИ.

10. Понятие и особенности утечки информации. Определение технического канала утечки информации. Структура, классификация, основные характеристики ТКУИ.

11. Выделенные (защищаемые) помещения. Характеристики речевого сигнала (звукового поля). Общая характеристика и классификация технических каналов утечки акустической (речевой) информации.

12. Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Способы и средства защиты вспомогательных технических средств и систем. Звукоизоляция помещений. Сертифицированные средства защиты.

13. Объекты вычислительной техники (автоматизированные системы). Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вы-

числительной техники и автоматизированными системами. Физическая природа побочных электромагнитных излучений.

14. Классификация способов и средств защиты объектов вычислительной техники (принципы построения, основные характеристики, требования по установке). Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Помехоподавляющие фильтры. Системы пространственного и линейного электромагнитного зашумления.

15. Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

16. Основные этапы проведения аттестации объектов информатизации по требованиям безопасности информации: задачи, содержание этапов, методы контроля и оценки состояния ТЗИ.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие : / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 (дата обращения: 01.09.2021). – Библиогр.: с. 213. – Текст : электронный.

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: 01.09.2021). – 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: 01.09.2021). – 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	Свободный доступ

		учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	
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 ос-

новного 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.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.