Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.41 Защита информации от утечки по техническим каналам»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2023

Рабочая программа дисциплины «*Б1.Д.Б.41 Защита информации от утечки по техническим каналам*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "9" марта 2023 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент — Н.П. Мошуров
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации 154961

© Мошуров Н.П, 2023
© ОГУ, 2023

1 Цели и задачи освоения дисциплины

Цель (цели) освоения 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:

− 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.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.28 Основы информационной безопасности*

Постреквизиты дисциплины: *Б1.Д.Б.37 Техническая защита информации*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9-В-1 Знает организацию защиты информации от утечки по техническим каналам в операционных системах, сетях и системах управления базами данных ОПК-9-В-2 Умеет формулировать и настраивать политику безопасности основных операционных систем, локальных компьютерных сетей, построенных на их основе, и систем управления баз данных	**Знать:** – способы перехвата информации в каналах утечки; – методы защиты информации от утечки по техническим каналам; – методы и методики контроля защищенности информации от утечки по техническим каналам; – средства контроля защищенности информации от утечки по техническим каналам; – отчетные

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		документы, оформляемые по результатам контроля защищенности информации от утечки по техническим каналам; **Уметь:** – проверять работоспособность средств защиты информации от утечки по техническим каналам, выполнение правил их эксплуатации; – 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:** – проведением контроля защищенности информации от утечки по техническим каналам; навыком подготовки отчетных материалов по результатам контроля защищенности информации от утечки по техническим каналам.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**216**	**216**
Контактная работа:	**90,25**	**90,25**
Лекции (Л)	46	46

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Лабораторные работы (ЛР)	44	44
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**125,75** *46* *50* *29,75*	**125,75** *46* *50* *29,75*
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение	12	2		2	8
2.	Технические каналы утечки информации	36	12		2	22
3.	Средства выявления каналов утечки информации	56	12		12	32
4.	Скрытие и защита информации от утечки по техническим каналам	44	12		2	30
5.	Методы и средства инженерной защиты и технической охраны объектов	40	6		14	20
6.	Технический контроль эффективности мер защиты информации	28	2		12	14
	Итого:	216	46		44	126
	Всего:	216	46		44	126

4.2 Содержание разделов дисциплины

№ 1 Введение

Виды, источники и носители защищаемой информации. Классификация иностранной технической разведки. Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Задачи систем защиты информации.

№ 2 Технические каналы утечки информации

Технические каналы утечки информации. Структура, классификация и основные характеристики. Технические каналы утечки информации, обрабатываемой ТСПИ. Электрические каналы утечки информации. Технические каналы утечки информации при передаче ее по каналам связи. Каналы утечки информации за счет паразитных связей. Электрические каналы утечки информации. Электромагнитные каналы утечки информации. Индукционный канал утечки информации. Технические каналы утечки речевой информации. Акустические каналы утечки речевой информации. Виброакустические технические каналы утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Оптико-электронный технический канал утечки речевой информации. Параметрические технические каналы утечки речевой информации. Технические каналы утечки видовой информации.

№ 3 Средства выявления каналов утечки информации

Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы спектра, радиочастотомеры. Многофункциональные комплекты для выявления каналов утечки информации. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М». Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья» Многофункциональный комплекс радиомониторинга и выявления каналов утечки информации «АРК-Д1ТИ. Комплекс «RS turbo3.8. Комплексы измерения ПЭМИН. Нелинейные локаторы. Комплекс для измерения характеристик акустических сигналов. Металлодетекторы. Портативная рентгенотелевизионная установка. Досмотровые эндоскопы.

№ 4 Скрытие и защита информации от утечки по техническим каналам

Экранирование электромагнитных волн. Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления. Фильтрация информационных сигналов. Пространственное и линейное зашумление. Способы предотвращения утечки информации через ПЭМИН ПК. Устройства контроля и защиты слаботочных линий и сети. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.

№ 5 Методы и средства инженерной защиты и технической охраны объектов

Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов. Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана.

№ 6 Технический контроль эффективности мер защиты информации

Цели и задачи технического контроля эффективности мер защиты информации. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний Порядок проведения контроля защищенности АС от НСД. Методы контроля побочных электромагнитных излучений генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	1	Организация аттестации выделенного помещения по требованиям безопасности информации	2
2.	2	Имитатор сигналов «Шиповник-2».	2
3.	3	Скоростной поисковый приемник радиосигналов «Скорпион»	2
4.	3	Работа с контрольным устройством «Тест»	2
5.	3	Многофункциональный поисковый прибор ST-031 «Пиранья»	4
6.	3	Поиск каналов утечки информации с помощью детектора поля DP- 20	2
7.	3	Поиск каналов утечки информации с помощью индикатора поля ST 110. Поиск и обнаружение радиозакладок в помещении	2
8.	4	Система виброакустической защиты (СВАЗ) Соната ИП-2.	2
9.	5	Установка и настройка ПАК «Соболь»	2
10.	5	Интеграция ПАК «Соболь» и Secret Net	2

11.	5	Настройка видеокомплекса BestDVR-801	4
12.	5	Dallas Lock 8.0-K программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов	4
13.	5	Система охранно-тревожной сигнализации. Система контроля и управления доступом.	2
14.	6	Система оценки защищенности выделенных помещений по акустическому и виброакустическому каналу «Шепот»	6
15.	6	Автоматизированная система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) «Сигурд».	6
		Итого:	44

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959

2. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328

5.2 Дополнительная литература

1. Торокин, А. А. Инженерно-техническая защита информации [Текст] : учеб.пособие для вузов / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 960 с.

2. Данилов, А. Н. Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366

3. Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 194 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4960

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва : Форум : ИНФРА-М, 2014. - 416 с. : ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3.

5. Проскурин, В. Г. Защита программ и данных [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 "Информационная безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем" / В. Г. Проскурин.- 2-е изд., стер. - Москва : Академия, 2012. - 208 с. : ил. - (Высшее профессиональное образование. Бакалавриат). - Библиогр.: с. 195-196. - ISBN 978-5-7695-9288-1.

5.3 Периодические издания

Журналы:
- InformationSecurity/Информационная безопасность;
- Проблемы информационной безопасности. Компьютерные системы;
- Защита информации. Инсайд;

– Специальная техника. БДИ" (Безопасность. Достоверность. Информация);
– Директор по безопасности;
– Разведка;
– Мир и безопасность.

5.4 Интернет-ресурсы

1. http://www.fsb.ru – сайт ФСБ РФ
2. http://www.fstec.ru – сервер ФСТЭК РФ
3. http://www.gov.ru – сервер органов государственной власти РФ
4. http://www.minsvyaz.ru – сайт министерства информационных технологий и связи РФ
5. http://www.scrf.gov.ru – сайт Совета Безопасности РФ
6. www.consultant.ru – Консультант плюс
7. https://gost.ru – Росстандарт
8. http://docs.cntd.ru – Электронный фонд правовой и нормативно-технической документации
9. http://www.securrity.ru – Сайт Информационная безопасность
10. https://www.securitylab.ru – Информационный портал по информационной безопасности
11. https://securelist.ru/ - Сетевая штаб-квартира экспертов «Лаборатории Касперского»
12. https://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle
13. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК: Защита информации.
14. https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii - «Coursera». Курсы, МООК: Методы и средства защиты информации
15. https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti - «Coursera». Курсы, МООК: Менеджмент информационной безопасности
16. https://www.intuit.ru/studies/courses/3648/890/info – «Интуит. Национальный открытый университет». Курсы, МООК: Аттестация объектов информатизации по требованиям безопасности информации.
17. https://www.intuit.ru/studies/courses/3649/891/info – «Интуит. Национальный открытый университет». Курсы, МООК: Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.
18. https://www.intuit.ru/studies/courses/2291/591/info – «Интуит. Национальный открытый университет». Курсы, МООК: Общие вопросы технической защиты информации
19. https://www.intuit.ru/studies/courses/3620/862/info – «Интуит. Национальный открытый университет». Курсы, МООК: Нормативно-методическое обеспечение технической зашиты информации

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Антивирусное ПО: Kaspersky Endpoint Security для бизнеса, имеется лицензия на 2 года использования, входит в Реестр отечественного ПО

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами, демонстрационным оборудованием. Компьютеры подключены к сети Интернет, обеспечен доступ в электронную информационно-образовательную среду университета. Во время лабораторных работ используется оборудование, закрепленное за кафедрой ВТ и ЗИ и КБиМОИС.