ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 16.09.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.42 Измерительная аппаратура контроля защищенности объектов информатизации
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 16.09.2021

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Антясов И. С.
Пользователь: antiasovis
Дата подписания: 16.09.2021

И. С. Антясов

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины является подготовка специалистов в области технической защиты информации и привитие навыков контроля работоспособности и эффективности применяемых технических средств защиты информации. Задачи дисциплины: изучение: - измерительной аппаратуры контроля защищённости технических каналов утечки информации; - методов контроля защищенности объектов информатизации; - методов анализа технических каналов утечки информации проектируемых и эксплуатируемых объектов информатизации; формирование у студентов навыков: - использования измерительной аппаратуры контроля защищенности объектов информатизации; - использования поисковой аппаратуры для обнаружения каналов передачи различных подслушивающих устройств.

Краткое содержание дисциплины

Цели и задачи контроля защищённости объектов информатизации. Измерительная аппаратура контроля защищённости технических каналов утечки информации. Активные и пассивные средства защиты информации. Правовые, нормативно-технические и организационные требования к измерительной аппаратуре контроля защищенности объектов информатизации. Акустический контроль защищенности. Виброакустический контроль защищенности. Контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок. Стендовые и объектовые специальные исследования. Альтернативные измерительные площадки Поисковые комплексы устройств негласного съема информации. Проверка измерительной аппаратуры.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать:средства защиты информации, используемые на критически важных объектах;
	Уметь:разрабатывать схемы проведения измерений;
	Владеть:навыками эксплуатации измерительной аппаратуры контроля защищенности объектов информатизации с учетом требований по обеспечению информационной безопасности
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Знать:технические каналы утечки информации; измерительную аппаратуру, применяемую для контроля защищённости объектов информатизации;
	Уметь:определять узлы автоматизированной системы для измерения параметров информативных сигналов технических средств обработки информации;
	Владеть:навыками проведения измерений физических параметров технических каналов утечки информации;

ПСК-3.1 способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	Знать:пассивные и активные способы защиты информации от утечки по техническим каналам;
	Уметь:обрабатывать и интерпретировать результаты измерений;
	Владеть:навыками применения методов математической обработки результатов измерений; навыками участия в экспертизе состояния защищенности информации на объекте защиты;

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.38 Основы радиотехники, Б.1.25 Техническая защита информации, Б.1.06 Физика	В.1.09 Обеспечение информационной безопасности на критически важных объектах, Производственная практика, преддипломная практика (10 семестр)

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.06 Физика	Знать физические основы возникновения технических каналов утечки информации. Уметь вычислять физические величины. Обладать навыками расчета и перевода физических единиц.
Б.1.25 Техническая защита информации	Знать технические каналы утечки информации. Уметь определять разведопасные направления. Обладать навыками применения технических средств защиты информации.
Б.1.38 Основы радиотехники	Знать основы радиотехники. Уметь выявлять избыточные элементы. Обладать навыками измерения вольтамперных характеристик

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	16	16

Самостоятельная работа (СРС)	60	60
Демаскирующие признаки устройств негласного съема информации	6	6
Методика проведения акустического и виброакустического контроля защищенности объектов информатизации	6	6
Обзор измерительной аппаратуры контроля защищенности объектов информатизации	8	8
Акустический канал утечки информации	6	6
Технические каналы утечки информации	12	12
Введение	6	6
Канал утечки за счет побочных электромагнитных излучений и наводок	10	10
Виброакустический канал утечки информации	6	6
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение	2	2	0	0
2	Измерительная аппаратура контроля защищённости технических каналов утечки информации	8	8	0	0
3	Средства защиты информации и демаскирующие признаки устройств негласного съема информации	12	8	0	4
4	Методики проведения акустического, виброакустического и за счет ПЭМИН контроля защищенности объектов информатизации	8	6	0	2
5	Поисковые комплексы контроля защищённости объектов информатизации	18	8	0	10

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение	2
2	2	Технические каналы утечки информации	2
3	2	Акустический канал утечки информации	2
4	2	Виброакустический канал утечки информации	2
5	2	Канал утечки за счет побочных электромагнитных излучений и наводок	2
6	3	Альтернативные измерительные площадки	2
7	3	Демаскирующие признаки устройств негласного съема информации	2
8	3	Пассивные средства защиты информации	2
9	3	Активные средства защиты информации.	2
10	4	Обзор измерительной аппаратуры контроля защищенности объектов информатизации	2
11	4	Методика проведения акустического и виброакустического контроля защищенности объектов информатизации	2
12	4	Методика проведения контроля защищенности объектов информатизации за счет обнаружения побочных электромагнитных излучений и наводок	2

13	5	Изучение комплекса «Навигатор»	2
14	5	Изучение комплекса «Спрут-мини»	2
15	5	Изучение комплекса «Пиранья»	2
16	5	Поверка измерительной аппаратуры	2

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	3	Поиск устройств негласного съема информации	2
2	3	Активные средства защиты информации	2
3	4	Поисковые мероприятия с помощью нелинейного локатора	2
4	5	Проведение акустического и виброакустического контроля защищенности объектов информатизации с помощью комплекса «Спрут-мини»	4
5	5	Проведение контроля защищенности объектов информатизации за счет обнаружения побочных электромагнитных излучений и наводок с помощью комплекса «Навигатор»	4
6	5	Поисковые мероприятия с помощью комплекса «Пиранья»	2

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение материалов по плану СРС	Дополнительная литература	60

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Использование проектно-организованных технологий обучения работе в команде над комплексным решением практических задач	Лабораторные занятия	Студенты делятся на несколько команд, каждая из которых прячет в кабинете иммитации закладных устройств, другая команда должна найти данные макеты	2

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Использование методов, основанных на изучении практики (case studies)	Применение комплексов «Пиранья», «Спрут-мини», «Навигатор»

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	текущий	1-15
Все разделы	ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	текущий	16-30
Все разделы	ПСК-3.1 способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	текущий	31-45
Все разделы	ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	итоговый	1-8
Все разделы	ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	итоговый	9-13
Все разделы	ПСК-3.1 способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	итоговый	14-20

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
текущий	Тестирование	Отлично: Выбраны все верные варианты Хорошо: Выбраны верные варианты, но есть замечания в ответах Удовлетворительно: Больше половины выбрано верных вариантов Неудовлетворительно: Меньше половины выбрано верных вариантов
итоговый	Зачет	Зачтено: Дан развернутый правильный ответ Не зачтено: Дан неверный ответ

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
текущий	тесты Измерительная.docx
итоговый	вопросы измерительная.docx

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Вестник УрФО. Безопасность в информационной сфере. — Челябинск: Изд. центр ЮУрГУ.

г) методические указания для студентов по освоению дисциплины:

1. Для Лабораторных работ
2. Антясов И.С. Измерительная аппаратура контроля защищенности объектов информатизации: методические указания к лабораторным работам.

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Технические средства и методы защиты информации. [Электронный ресурс] : учеб. пособие / А.П. Зайцев [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: http://e.lanbook.com/book/5154 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Основная литература	Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 15.09.2021). — Режим доступа:	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

		для авториз. пользователей.		
3	Основная литература	Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам : справочное пособие / Г. А. Бузов. — Москва : Горячая линия-Телеком, 2018. — 586 с. — ISBN 978-5-9912-0424-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111027 (дата обращения: 15.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Лабораторные занятия	910 (3б)	Комплект компьютерного оборудования, Стенд по методам и средствам защиты телефонных аппаратов и телефонных линий, Стенд по биометрическим способам индикации, Стенд по противопожарной защите, Стенд по системам аналогового видеонаблюдения, Стенд по системам цифрового видеонаблюдения, Стенд по техническим средствам охраны на базе приборов «Сигнал 20» и «Сигнал 20 П», Стенд по техническим средствам охраны на базе контроллера «С200-КФЛ», Переносной комплекс для измерений «Навигатор П3Г», Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А», Лабораторный стенд для исследования линий связи, Селективный микровольтметр, Осциллограф С1-65, Генератор импульсов Г5-54, Аппаратный шифратор, Поисковый комплекс «Пиранья», Нелинейный локатор «Родник-2К», Детектор поля, Устройство комбинированной защиты, настенные информационные стенды (3 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Орион, VidioNET.