УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол №_5/24__
Председатель _____Волков М.А._
«_21_» ____05_ _____ 2024_ _____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Защита информации от утечки по техническим каналам**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	3

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент, Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Учебная дисциплина «Защита информации от утечки по техническим каналам» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью освоения дисциплины «Защита информации от утечки по техническим каналам» является формирование у студентов знаний по основам технической защиты информации, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач технической защиты информации с учетом требований системного подхода.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- по концепции и организационным основам инженерно-технической защиты информации;

- теоретическим и физическим основам технической защиты информации;

- по техническим средствам добывания и защиты информации;

- по методическому обеспечению технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации от утечки по техническим каналам» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-5, ОПК-6, ОПК-9.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Программно-аппаратные средства защиты информации, Методы и средства криптографической защиты информации, Сети и системы передачи информации, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Научно-исследовательская работа, Защита информации от утечки по техническим каналам, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Управление информационной безопасностью, Организационное и правовое обеспечение информационной безопасности, Ознакомительная практика, Теория информации, Основы информационной безопасности.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	**знать**: основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **уметь**: решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **владеть**: навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	**знать**: методические документы, регламентирующие деятельность по защите информации **уметь**: применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации **владеть**: навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	**знать**: порядок организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **уметь**: организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **владеть**: навыками организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 5 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 180 часов

Форма обучения: очная

Вид учебной работы	**Количество часов (форма обучения очная)**	
	Всего по плану	**В т.ч. по семестрам**
		6
1	**2**	**3**
Контактная работа обучающихся с преподавателем в соответствии с УП	72	72
Аудиторные занятия:	72	72
Лекции	18	18
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	36	36
Самостоятельная работа	72	72
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование, Оценивание реферата	Тестирование, Оценивание реферата
Курсовая работа	Курсовая работа	Курсовая работа
Виды промежуточной аттестации (экзамен, зачет)	Экзамен (18)	Экзамен
Всего часов по дисциплине	180	180

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	**Всего**	**Виды учебных занятий**					**Форма текущего контроля знаний**
		Аудиторные занятия			**Занятия в интерактивной форме**	**Самостоятельная работа**	
		Лекции	**Практические занятия, семинары**	**Лабораторные работы, практикумы**			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Раздел 1. Основы технической защиты информации							
Тема 1.1. Концепция технической защиты информации	8	2	2	0	0	4	Вопросы к Экзамену, Тестирование, Оценивание реферата

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 1.2. Физические основы утечки информации за счет побочных излучений и наводок	10	2	4	0	0	4	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 1.3. Основные направления технической защиты ин-формации в организации	6	2	0	0	0	4	Вопросы к Экзамену, Тестирование, Оценивание реферата
Раздел 2. Технические каналы утечки информации							
Тема 2.1. Типовая структура и виды технических каналов утечки информации	8	2	2	0	0	4	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.2. Акустические, виброакустические и оптические каналы утечки инф ор-мации.	8	2	2	0	0	4	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 2.3. Электромагнитные каналы утечки	8	2	2	0	0	4	Вопросы к Экзамену, Тестирование, Оценивани

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
информации, образуемые средствами вычислительной техники.							е реферата
Раздел 3. Методы и средства защиты информации от утечки по техническим каналам							
Тема 3.1. Методы и средства защиты информации от утечки в электромагнитном канале	32	2	2	12	0	16	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 3.2. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале.	18	2	2	6	0	8	Вопросы к Экзамену, Тестирование, Оценивание реферата
Тема 3.3. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств	46	2	2	18	0	24	Вопросы к Экзамену, Тестирование, Оценивание реферата
Итого подлежит	144	18	18	36	0	72	

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
изучению							

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы технической защиты информации

Тема 1.1. Концепция технической защиты информации

Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам. Концепция технической защиты информации. Основные положения системного подхода к технической защите информации. Модель системы защиты информации (СЗИ).

Тема 1.2. Физические основы утечки информации за счет побочных излучений и наводок

Функциональные и случайные опасные сигналы. Источники опасных сигналов. Побочные электромагнит¬ные излучения и наводки (ПЭМИН) как физическая основа возникновения случайных опасных сигналов. Побочные преобразования акустических сигналов в электрические. Паразитные связи и наводки. Низкочастотные и высокочастотные излучения технических средств. Электромагнитные излучения сосредоточенных и распределённых источников. Утечка информации по цепям электропитания. Утечка информации по цепям заземлений.

Тема 1.3. Основные направления технической защиты ин-формации в организации

Основные факторы обеспечения защиты информации от угроз утечки информации. Этапы процесса утечки информации. Основные направления защиты: физическая защита; скрытие информации; нейтрализация источников опасных сигналов. Основные методы технической защиты информации: инженерная защита; техническая охрана объектов; пространственное (структурное, временное и энергетическое) скрытие.

Раздел 2. Технические каналы утечки информации

Тема 2.1. Типовая структура и виды технических каналов утечки информации

Типовая структура и виды технических каналов утечки информации (ТКУИ). Классификация ТКУИ. Основные показатели ТКУИ.

Тема 2.2. Акустические, виброакустические и оптические каналы утечки инфор-мации.

Понятие и основные характеристики акустического, виброакустического и оптического каналов утечки информации. Пассивные и активные способы защиты информации в выделенных помещениях от несанкционированного прослушивания. Рекомендации по выбору систем акустической и виброакустической защиты. Характеристика и противодействие оптическим каналам утечки информации. Средства противодействия наблюдению в оптическом диапазоне.

Тема 2.3. Электромагнитные каналы утечки информации, образуемые средствами вычислительной техники.

Характеристика режимов обработки информации в ПЭВМ с точки зре¬ния утечки информации. Режим вывода информации на экран монитора. Потенциально информативные и неинформативные излучения. Условия возникновения элек-тромагнитного канала утечки информации. Электрические каналы утечки ин¬формации. Сосре¬доточенные и распределённые случайные антенны. Специально создаваемые техниче¬ские каналы утечки информации. Аппаратные закладки для перехвата изображений, выводимых на экран монито¬ра. Аппаратные закладки для перехвата информации, записываемой на жёсткий диск. Программные закладки.

Раздел 3. Методы и средства защиты информации от утечки по техническим каналам

Тема 3.1. Методы и средства защиты информации от утечки в электромагнитном канале

Методы пассивной и активной защиты. Экранирование, зашумление и фильтрация опасных сигналов. Методы и средства измерения уровня защищённости от утечки по электромагнитному каналу

Тема 3.2. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале.

Методы пассивной и активной защиты. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу. Средства противодействия перехвату «информации по акустовибрационному каналу.

Тема 3.3. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств

Средства технической разведки. Мероприятия по выявлению средств технической разведки. Специальные технические средства (СТС). Методика поиска СТС. Радиомониторинг. Локализация радиоизлучающих СТС. Проверка наличия инфракрасных (ИК) излучений. Выявление низкочастотных (НЧ) магнитных полей. Проверка электросети и телефонных коммуникаций. Проверка помещения на наличие акустических каналов утечки. Физический поиск СТС.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Основы технической защиты информации

Тема 1.1. Концепция технической защиты информации

Вопросы к теме:

Очная форма

1. Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам.
2. Концепция технической защиты информации.
3. Основные положения системного подхода к технической защите информации.
4. Модель системы защиты информации (СЗИ).

Тема 1.2. Физические основы утечки информации за счет побочных излучений и наводок

Вопросы к теме:

Очная форма

1. Опасные сигналы и их источники.
2. Побочные электромагнитные излучения и наводки.

Раздел 2. Технические каналы утечки информации

Тема 2.1. Типовая структура и виды технических каналов утечки информации

Вопросы к теме:

Очная форма

1. Типовая структура и виды технических каналов утечки информации.
2. Классификация технических каналов утечки информации.
3. Основные показатели технических каналов утечки информации.

Тема 2.2. Акустические, виброакустические и оптические каналы утечки инфор-мации.

Вопросы к теме:

Очная форма

1. Характеристика и противодействие акустическим каналам утечки информации.
2. Характеристика и противодействие оптическим каналам утечки информации.

Тема 2.3. Электромагнитные каналы утечки информации, образуемые средствами вычислительной техники.

Вопросы к теме:

Очная форма

1. Характеристика режимов обработки информации в ПЭВМ с точки зре¬ния утечки информации.
2. Потенциально информативные и неинформативные излучения.
3. Электрические каналы утечки ин¬формации.
4. Специально создаваемые техниче¬ские каналы утечки информации.

Раздел 3. Методы и средства защиты информации от утечки по техническим каналам

Тема 3.1. Методы и средства защиты информации от утечки в электромагнитном канале

Вопросы к теме:

Очная форма

1. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале.
2. Экранирование, зашумление и фильтрация опасных сигналов.

Тема 3.2. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале.

Вопросы к теме:

Очная форма

1. Методы пассивной и активной защиты.
2. Технические средства обнаружения утечки инфор¬мации по акустическому (виброакустическому) каналу.
3. Средства противодействия перехвату «информации по акустовибрационному каналу.

Тема 3.3. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Защита каналов передачи информации генератором шума «Гром-ЗИ-4»
Цели: Ознакомление с техническими характеристиками генератора шума «Гром-ЗИ-4», изучение правил его эксплуатации и получение практических навыков работы с генератором шума Гром-ЗИ-4»

Содержание: При подготовке к использованию прибора по назначению необходимо выполнить следующие операции: - подключить антенну к прибору. Антенная система генератора шума "ГРОМ-ЗИ-4" излучает электромагнитное поле шума с поляризацией, близкой к эллиптической. При использовании "ГРОМ-ЗИ-4" дли зашумления малогабаритных, локально размещенных объектов, антенная система может не ориентироваться в про¬странстве. При зашумлении крупногабаритных объектов (вычислительных центров, терминальных залов мощных вычислительных комплексов) рекомендуется использовать несколько комплектов "ГРОМ-ЗИ-4", размещая антенные системы в трех перпендикулярных плоскостях; - подключить телефонный аппарат (ТА) и линию к гнездам "ТА" и "ЛИНИЯ" прибора; - подключить прибор к электросети 220 В 50 Гц. - включить прибор клавишей "СЕТЬ" и проконтролировать включение по индикатору.
Результаты: Ознакомиться с техническими характеристиками генератора шума «Гром-ЗИ-4», изучить правила его эксплуатации и получить практические навыки работы; составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10730
Ознакомление с техническими характеристиками селективного микровольтметра В6-9
Цели: Получение практических навыков в работе с селективным микровольтметром в ходе измерения опасных сигналов
Содержание: Перед проведением измерений подготовьте прибор к работе в соответствии с инструкцией по эксплуатации. Подключите к телефонной линии низкочастотную радиозакладку (с рабочей частотой до100 кГц) в режиме микрофона. Подключите микровольтметр к линии и убедитесь в работе закладки путем измерения уровня опасного сигнала в линии в широкополосном режиме. Переведите микровольтметр в селективный режим работы и путем сканирования частотного диапазона найдите максимум опасного сигнала. Для контроля частоты измеряемого сигнала к выходному гнезду микровольтметра с помощью соединительного кабеля подключайте частотомер, а для наблюдения формы сигнала – осциллограф. На основе проведения ряда измерений на близких частотах строится спетрально-энергетическая характеристика закладки. Аналогичным методом исследуются характеристики случайных (паразитных) микрофонов. Хорошие результаты получаются при исследовании динамических громкоговорителей, входящих в состав систем радиотрансляции, оповещения, диспетчерской связи и т.п.
Результаты: Научиться определять спектрально-энергетические характеристики случайных микрофонов; получить практические навыки работы с селективным микровольтметром В6-9; составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10730
Исследование акустического зашумления помещения
Цели: Исследование возможностей генератора шума SI-3010, получение практических навыков в работе по акустическому зашумлению помещения
Содержание: Для защиты от утечки информации по вибрационному каналу через стены и перекрытия целесообразно использовать электромагнитные излучатели типа «TRN-2000» (или аналогичные). Ра¬диус защиты излучателя «TRN-2000» порядка 6 м, одного излучателя достаточно для обеспечения виб¬роакустической защиты стены длиной 10 м, в случае его размещения в центре стены. При расположении излучателя вблизи места соединения двух стен площадь защищаемой поверхности уменьшается. В случае установки одного излучателя в центре защи¬щаемой конструкции (например, стены) в данном помещении могут возникнуть значительные паразитные акустические шумы. Для защиты от утечки информации по вибрационному каналу через стекла, зеркала и другие тонкие отражающие поверхности целесообразно использовать виброакустические преобразователи «ВД-1». На каждом элементе остекления должно быть установлено не менее

одного излучателя в соответствии с их радиусом действия, но не ближе 50 см от края защищаемого элемента остекления. Излучатели устанав¬ливаются на стекла с помощью двустороннего скотча или быстросохнущего клея. Для защиты от утечки информации по вибрационному каналу через инженерные коммуникации, трубы и батареи отопления, водопроводные трубы, деревянные или металлические двери и т.д. целесооб¬разно использовать излучатели «ВД-1». Для защиты инженерных коммуникаций излучатели закрепляют¬ся на трубах с помощью специальных скоб или хомутов и располагаются в непосредственной близости от мест выхода этих труб за пределы защищаемого помещения. Для защиты от утечки информации по акустическому каналу через воздуховоды, открытые окна, двери и т.д. целесообразно использовать акустические излучатели типа «OMS-2000» или аналогичные. Подключение одного акустического излучателя типа «OMS-2000» к прибору обеспечивает эффективную защиту помещения объемом 60 м3. В вентиляционных коробах акустические излучатели размещаются внутри короба в непосредственной близости от мест его выхода из защищаемого помещения. В тамбурах дверных проемов акустические излучатели располагаются в местах, удобных для их монтажа и подключения. При установке нескольких одинаковых излучателей на одну защищаемую поверхность рекомендуется включать излучатели синфазно. После подключения излучателей подключите прибор к электросети 220 В, включите его кнопкой «СЕТЬ» и проконтролируйте включение по индикатору «СЕТЬ». Установите с помощью регуляторов «Уровень шума» необходимый уровень шумовой помехи. С помощью регуляторов «АЧХ» установите необходимый спектр шумовой помехи. Для формирования речеподобной или внешней помехи к гнезду «Вход» 3-го канала необходимо под¬ключить внешний источник помехи (например, диктофон). Проведите измерения уровня акустического сигнала при выключенном генераторе шума и уровня шума. Дайте оценку эффективности зашумления по изученной ранее методике.

Результаты: Исследовать возможности генератора шума SI-3010; получить практические навыки в работе по акустическому зашумлению помещения; составить отчет о проделанной работе и отчитаться по нему у преподавателя.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10730

ОБНАРУЖЕНИЕ И ЛОКАЛИЗАЦИЯ ПЕРЕДАЮЩИХ РАДИОСРЕДСТВ С ПОМОЩЬЮ ДЕТЕКТОРА ПОЛЯ D 006

Цели: Ознакомление с техническими характеристиками изделия D 006, изучение правил его эксплуатации, получение практических навыков работы с изделием.

Содержание: Работа проводится в игровом варианте попарно в два этапа. Первый студент – «злоумышленник» (З), второй – сотрудник службы безопасности (СБ). На первом этапе З изучает технические характеристики и правила эксплуатации многофункционального имитатора ИМФ-2, а СБ – технические характеристики, правила эксплуатации и методику поиска радиозакладок с помощью детектора поля D 006 (описания приводятся ниже). Перед началом практических действий оба игрока отвечают на контрольные вопросы преподавателя с целью проверки уровня их подготовки. После этого З включает ИМФ-2 в требуемом режиме, а СБ осуществляет открытый «поиск», чтобы уяснить особенности использования D 006. Затем, СБ на некоторое время (1…2 мин) покидает аудиторию. За это время З должен включить ИМФ-2 в режим радиозакладки и где-либо замаскировать или спрятать в личных вещах присутствующих в аудитории студентов. Для создания акустического фона, вызывающего функционирование ИМФ-2 может использоваться магнитофонная запись или доклад одного из присутствующих студентов. Вошедший в аудиторию СБ начинает поиск радиозакладки с использованием D 006. При этом фиксируется время начала и окончания поиска. На втором этапе игроки меняются ролями. Аналогично работает вторая и последующие пары игроков в группе. Победители определяются в двух номинациях: среди

сотрудников службы безопасности и «злоумышленников». В первом случае лучшим признается тот студент, который затратил минимальное время на обнаружение и локализацию радиозакладки, во втором – тот, чью закладку искали максимальное время. Выполнение работы оценивается «зачет» – «не зачет».
Результаты: В результате выполнения работы студент должен изучить технические характеристики изделия D 006, правила его эксплуатации, получить практические навыки работы с изделием, составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10730
Обнаружение радиозлучающих устройств с использованием сканирующего радиоприемника AR-3000A
Цели: Ознакомление с техническими характеристиками изделия AR-3000A, изучение правил эксплуатации изделия, получение основных практических навыков работы с изделием.
Содержание: - Подключите подходящую антенну к байонетному гнезду на задней панели приёмника. - Подключите AR3000A к источнику питания постоянного тока, используя прилагаемые сетевой адаптер или кабель питания. Ни в коем случае не подключайте приёмник к бытовой электросети. - Перед включением питания установите регулятор громкости в положение 10 часов, регулятор порога схемы БШН в положение 12 часов и убедитесь, что расположенный на задней панели переключатель дистанционного управления через RS232C находится в положении «OFF». - Нажмите клавишу включения питания. Убедитесь, чтобы при этом на дисплее не отобразилось ни одного из следующих индикаторов: <KEYLOCK>, <RMT> и <PAUSE>. Если они отображаются на дисплее сотрите их. После выполнения вышеизложенного приёмник готов к вводу частоты и режима. При подготовке к использованию прибора по назначению необходимо выполнить следующие операции: - Подсоедините соответствующую антенну к байонетному разъему на задней панели. - Подсоедините к приемнику нужный источник питания, используя либо данный блок питания, либо 12-ти вольтовой кабель. - После включения установите уровень громкости в положение «10», ручку бесшумной настройки в положение 12 и убедитесь, что переключатель дистанционного управления в положении (OFF). - Включите питание. Убедитесь, что ни один из указанных символов <KEYLOCK>, <RMT>, <PAUSE> не появился на ЖКИ-дисплее при первом включении. - Уберите эти символы с дисплея при их появлении как указано выше. - После указанной процедуры приемник готов к вводу частоты и режима приема. Основные действия в каждом отдельном режиме приема Режим ввода: - В этом режиме можно выбрать частоту для немедленного прослушивания, ввод частоты произойдет после нажатия кнопки (DIAL). Выбор частоты приема можно осуществить с помощью десятичных кнопок, кнопок (UP/DOWN) или ручки настройки. Прямой ввод с помощью кнопок: Выберите частоту коммерческого авиационного диапазона 133,7 МГц в режиме AM. - Нажмите [DIAL]. - Нажмите [MODE]. Нажмите [UP/DOWN] или поверните ручку настройки, пока на ЖКД не появится индикатор <AM>. Нажмите [ENTER]. - Последовательно нажмите клавиши [STEP] [2] [5] [ENTER]. В данном случае в этом нет необходимости, однако тем самым Вы установите разнос между каналами в 25 кГц, предусмотренный для коммерческого авиационного диапазона, и приемник в дальнейшем будет точно настраиваться на другие станции при вращении ручки настройки. Если Вы желаете прослушивать только частоту 133,7 МГц без дальнейшей перестройки, этот пункт может быть опущен. - Последовательно нажмите клавиши [1] [3] [3] [.] [7] [ENTER]. Теперь приемник точно настроен на частоту 133,7 МГц в режиме AM. Если при наборе частоты Вы допустили ошибку, нажмите клавишу [ENTER] и начните набор сначала. Режим программного поиска в диапазоне 118-138 МГц с шагом 25 кГц, в режиме AM: - Нажмите последовательно [2nd F] [SEARCH SET]. На дисплее появится мигающий символ <SEARCH>. Кнопкой [UP/DOWN] установите режим AM,

затем нажмите клавишу [ENTER]. - На дисплее появится мигающий символ <STEP>. Нажмите [2] [5] [ENTER], чтобы установить шаг, равный 25 кГц. - На дисплее появится символ <L> - приемник запрашивает нижнюю (исходную) частоту. Нажмите [1] [1] [8] [ENTER]. - На дисплее появится символ <H> - приемник запрашивает верхнюю (конечную) частоту. Нажмите [1] [3] [8] [ENTER]. На дисплее появится символ <P>, приемник автоматически начинает поиск. При обнаружении сигнала - поиск приостановится. Для его возобновления, пока присутствует сигнал, Вы можете слегка покрутить ручку настройки или нажать [UP/DOWN]. - Для прекращения программного поиска нажмите [SEARCH], для его возобновления повторно нажмите [SEARCH]. Введенные Вами параметры занесены в память, они не пропадут даже при выключении приемника. Чтобы вести поиск в имеющихся в памяти диапазонах, выберите соответствующий диапазон и нажмите [SEARCH]. Полное описание практических действий изложено в технической документации на поисковый приёмник AR3000A.

Результаты: Ознакомиться с техническими характеристиками всеволнового приёмника «AR-3000A»; изучить правила его эксплуатации и получить практические навыки работы; составить отчёт о проделанной работе и защитить его у преподавателя.

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10730

Изучение методов поиска и локализации специальных технических средств с использованием прибора ST-032 Пиранья

Цели: Изучить возможности прибора ST 032 «Пиранья» и научиться осуществлять поиск и локализацию специальных технических средств несанкционированного получения информации

Содержание: Многофункциональный поисковый прибор ST 032 «Пиранья» предназначен для проведения мероприятий по обнаружению и определению местоположения специальных технических средств (СТС) негласного получения информации, для выявления естественных и искусственно созданных каналов утечки информации, а также для контроля качества защиты информации. С использованием прибора ST 032 возможно решение следующих контрольно-поисковых задач: - обнаружение и определение местоположения радиоизлучающих СТС (РСТС); - обнаружение и определение местоположения СТС, работающих с излучением в инфракрасном диапазоне; - обнаружение и определение местоположения СТС, использующих для передачи информации проводные линии различного предназначения; - обнаружение и определение местоположения источников магнитных полей, а также исследование технических средств, обрабатывающих речевую информацию. - выявпение наиболее уязвимых мест, с точки зрения возникновения виброакус-тических каналов утечки информации, и оценка эффективности систем вибро-акустической защиты помещений. - выявление наибопее уязвимых мест, с точки зрения возникновения каналов утечки акустической информации, и оценка эффективности звукоизоляции помещений. Работа проводится в игровом варианте попарно в два этапа. Первый студент – «злоумышленник» (З), второй – сотрудник службы безопасности (СБ). На первом этапе З изучает технические характеристики и правила эксплуатации многофункционального имитатора ИМФ-2, а СБ – технические характеристики, правила эксплуатации и методику поиска каналов утечки информации с помощью поискового комплекса «Пиранья ST-032». Перед началом практических действий оба игрока отвечают на контрольные вопросы преподавателя с целью проверки уровня их подготовки. Контрольные вопросы приведены ниже. Затем, СБ на некоторое время (1…2 мин) покидает аудиторию. За это время З должен включить ИМФ-2 в режим радиозакладки и где-либо замаскировать или спрятать в личных вещах присутствующих в аудитории студентов. Для создания акустического фона, вызывающего функционирование ИМФ-2 может использоваться магнитофонная запись или доклад одного из присутствующих студентов. Вошедший в аудиторию СБ начинает поиск радиозакладки с использованием ST-032. При этом фиксируется время начала и

окончания поиска. На втором этапе игроки меняются ролями.
Результаты: Изучить прибор ST 032 «Пиранья» и основные методы поиска и локализации специальных технических средств несанкционированного получения информации; составить отчет о проделанной работе и отчитаться по нему у преподавателя. При этом студент должен продемонстрировать: освоение управления прибором во всех предусмотренных режимах его работы; знание подготовительного этапа контрольно-поисковых работ заданном помещении; навыки поиска специальных технических средств несанкционированного получения информации.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10730

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы рефератов

Тема 1. Основные показатели эффективности добывания информации
Тема 2. Способы и средства дезинформирования при противодействии радиолокационному наблюдению
Тема 3. Скремблеры как техническое средство защиты информации
Тема 4. Способы и средства дезинформирования при противодействии радиолокационному наблюдению
Тема 5. Сравнительный анализ характеристик средств обнаружения радиозакладок
Тема 6. Способы и средства дезинформирования при противодействии радиолокационному наблюдению
Тема 7. Классификация способов нейтрализации закладных устройств
Тема 8. Требования к цепям заземления и способы их реализации
Тема 9. Характеристики экранов, влияющие на эффективность электромагнитного экранирования
Тема 10. Сравнительный анализ характеристик средств обнаружения радиозакладок
Тема 11. Скремблеры как техническое средство защиты информации
Тема 12. Сравнительный анализ характеристик средств обнаружения радиозакладок
Тема 13. Характеристики экранов, влияющие на эффективность электромагнитного экранирования
Тема 14. Характеристики экранов, влияющие на эффективность электромагнитного экранирования
Тема 15. Условия и способы эффективного акустического зашумления речевой информации в помещении

Темы курсовой работы

Тема 1. Разработка автоматизированной обучающей системы по использованию нормативных правовых актов ФСТЭК, регламентирующих деятельность по защите информации
Тема 2. Разработка автоматизированной обучающей системы по использованию нормативных правовых актов ФСТЭК, регламентирующих деятельность по защите информации от утечки по техническим каналам
Тема 3. Анализ электромагнитных каналов утечки информации в автоматизированной системе
Тема 4. Анализ акустических каналов утечки информации в автоматизированной системе
Тема 5. Анализ эффективности использования физических средств защиты в автоматизированной системе
Тема 6. Принципы обнаружения и локализации радиозакладок
Тема 7. Сравнительный анализ характеристик средств обнаружения радиозакладок
Тема 8. Обеспечение защиты от оптических каналов утечки информации

Тема 9. Реализация защиты информации от утечки посредством ЭМИН
Тема 10. Предотвращение утечки информации по цепям электропитания и заземления
Тема 11. Способы увеличения дальности скрытного наблюдения в оптическом видимом и инфракрасном диапазонах
Тема 12. Обеспечение энергетического скрытия речевой информации в телефонных линиях связи и принципы их решения

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Обобщённая структура государственной системы защиты информации.Основные документы по противодействию иностранным техническим разведкам
2. Концепция технической защиты информации
3. Основные положения системного подхода к технической защите информации
4. Модель системы защиты информации
5. Опасные сигналы (функциональные и случайные) и их источники
6. Побочные электромагнитные излучения и наводки. Побочные преобразования акустических сигналов в электрические сигналы
7. Побочные электромагнитные излучения и наводки. Паразитные связи и наводки
8. Побочные электромагнитные излучения и наводки.Низкочастотные и высокочастотные излучения технических средств
9. Побочные электромагнитные излучения и наводки. Электромагнитные излучения сосредоточенных и распределённых источников
10. Побочные электромагнитные излучения и наводки.Утечка информации по цепям электропитания и заземления
11. Основные факторы обеспечения защиты информации от угроз утечки информации
12. Классификация направлений и методов инженерно-технической защиты информации
13. Типовая структура и виды технических каналов утечки информации
14. Классификация технических каналов утечки информации
15. Основные показатели технических каналов утечки информации
16. Характеристика и противодействие акустическим каналам утечки информации. Пассивные и активные способы защиты речи от несанкционированного прослушивания
17. Характеристика и противодействие оптическим каналам утечки информации. Пассивные и активные способы защиты информации от несанкционированного наблюдения
18. Характеристика режимов обработки информации в ПЭВМ с точки зрения утечки информации
19. Потенциально информативные и неинформативные излучения
20. Электрические каналы утечки информации
21. Специально создаваемые технические каналы утечки информации
22. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале
23. Экранирование, зашумление и фильтрация опасных сигналов
24. Методы и средства измерения уровня защищённости от утечки по электромагнитному каналу
25. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу
26. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу
27. Средства противодействия перехвату «информации по акустовибрационному каналу

28. Средства противодействия перехвату «информации по акустовибрационному каналу
29. Специальные технические средства (СТС). Методика поиска СТС
30. Технические средства для проведения радиомониторинга помещений
31. Приборы для выявления акустических (виброакустических) каналов утечки
32. Досмотровая техника для осуществления физического поиска специальных технических средств (СТС).

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Основы технической защиты информации			
Тема 1.1. Концепция технической защиты информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Тема 1.2. Физические основы утечки информации за счет побочных излучений и наводок	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Тема 1.3. Основные направления технической защиты ин-формации в организации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Раздел 2. Технические каналы утечки информации			
Тема 2.1. Типовая структура и виды технических каналов утечки информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 2.2. Акустические, виброакустические и оптические каналы утечки инфор-мации.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Тема 2.3. Электромагнитные каналы утечки информации, образуемые средствами вычислительной техники.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Раздел 3. Методы и средства защиты информации от утечки по техническим каналам			
Тема 3.1. Методы и средства защиты информации от утечки в электромагнитном канале	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	16	Тестирование, Оценивание реферата
Тема 3.2. Методы и средства защиты информации от утечки в акустическом (виброакустическом) канале.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование, Оценивание реферата
Тема 3.3. Мероприятия по выявлению средств технической разведки. Методика поиска специальных технических средств	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	24	Тестирование, Оценивание реферата

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы
основная

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов ; Душкин А.В.; Барсуков О.М.; Кравцов Е.В.; Славнов К.В. - Москва : Горячая линия - Телеком, 2016. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204705.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0470-5. / .— ISBN 0_250838

2. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам : учебное пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2015. - 586 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204248.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0424-8. / .— ISBN 0_251025

дополнительная

1. Груздева Л. М. Защита информации : учебное пособие / Л. М. Груздева ; Груздева Л. М. - Москва : РУТ (МИИТ), 2019. - 144 с. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции РУТ (МИИТ) - Информатика. - Режим доступа: ЭБС "Лань"; для авторизир. пользователей. - ISBN 978-5-7876-0326-2. / .— ISBN 0_399559

2. Внуков Андрей Анатольевич. Защита информации : Учебное пособие для вузов / А.А. Внуков ; Внуков А. А. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2021. - 161 с. - (Высшее образование). - URL: https://urait.ru/bcode/470131 (дата обращения: 26.10.2021). - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-07248-8 : 539.00. / .— ISBN 0_295589

3. Внуков Андрей Анатольевич. Защита информации в банковских системах : Учебное пособие для вузов / А.А. Внуков ; Внуков А. А. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 246 с. - (Высшее образование). - URL: https://urait.ru/bcode/490278 (дата обращения: 24.01.2022). - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-01679-6 : 649.00. / .— ISBN 0_316671

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Защита информации от утечки по техническим каналам» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов ; УлГУ, ФМИиАТ. - 2021. - 21 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10730. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_261316.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Альт рабочая станция
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») :

электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового

проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доцент, Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО