Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

С.Т. Князев
27 апреля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156878

Модуль
Технические средства и методы защиты информации

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП 10.05.02/22.01**
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** *10.05.02*

Области образования, в рамках которых реализуется модуль образовательной программы по ФГОС ВО 3++ *специалитет*

№ п/п	Перечень областей образования, для которых разработан ФГОС ВО 3++	Уровень подготовки
1.	Инженерное дело, технологии и технические науки	*специалитет*

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	д.т.н., профессор	Директор УНЦ ИБ	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Руководитель модуля - *С.В. Поршнев*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Технические средства и методы защиты информации

1.1. Аннотация содержания модуля

Модуль «Технические средства и методы защиты информации» содержит дисциплин, усвоение которых позволяет обучаемым обеспечить безопасность объекта в случае физического проникновения нарушителей, негласного прослушивания информации, при попытках использования внешних средств технической разведки, и при использовании противником технических каналов утечки информации. Значительное внимание уделяется электромагнитному каналу утечки информации, теории распространения, рассеяния, интерференции и дифракции электромагнитных волн радиодиапазона.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах
1	Средства технической разведки	*4/144*
2	Техническая защита информации	*4/144*
3	Технические каналы утечки информации	*5/180*
4	Технические средства охраны	*4/144*
	ИТОГО по модулю:	*17/612*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	*Гуманитарные аспекты информационной безопасности* *Информационные технологии* *Безопасность баз данных* *Компьютерное моделирование* *Основы технической защиты информации*
Постреквизиты и корреквизиты модуля	*Информационные технологии* *Безопасность жизнедеятельности* *Управление информационной безопасностью* *Защита информации в информационно-управляющих систем* *Основы научных исследований* *Защита информации* *Методы и системы обнаружения компьютерных атак* *Защита информации в объектах критической информационной инфраструктуры (КИИ)* *Методы анализа сигналов систем* *Проектирование защищенных телекоммуникационных систем*

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям. Результаты обучения формулируются глаголами в активной форме или отглагольным существительным, должны содержать индикатор/измеряемый критерий (например, самостоятельно формулировать предложения…; понимать/понимание; рассчитывать необходимое количество материалов…/ расчет необходимого количества материалов… и т.д.). При выборе глаголов полезно опираться на таксономию Блума.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 2

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)			
	Знания:	**Умения:**	**Практический опыт, владение**	**Другие результаты** *(указываются при необходимости, к примеру,* ***личностные качества****)*
ОПК-11. Способен применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки	"РО1-З ОПК11 Знает положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования"	"РО1-У ОПК11 Умеет применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования"	"РО1-В ОПК11 Владеет методами анализа и синтеза для решения профессиональных задач"	

сигналов для решения задач профессиональной деятельности				

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
Технические средства и методы защиты информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1
Средства технической разведки

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1 ~~(электив, майнор)~~*~~[наименование]~~*

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Основы управления информационной безопасностью	Основы управления информационной безопасностью Элементы разработки СУИБ в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах
~~**2**~~	Стандартизация в области управления информационной безопасностью	Основные международные и национальные стандарты в области управления информационной безопасностью на основе информационной системы. Стандарты на основе «Общих критериев»
~~**3**~~	Управление информационными рисками как базовый процесс функционирования СУИБ	Управление информационными рисками как базовый процесс функционирования СУИБ Математические модели и методы управления информационными рисками

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

1. Курило А.П. Основы управления информационной безопасностью : учебное пособие для вузов. — 2-е изд., испр. / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — М. : Горячая линия-Телеком, 2014. — 244 с.: ил. — (Вопросы управления информационной

безопасностью. Выпуск 1).

2. Милославская Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов. — 2-е изд., испр. / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — М. : Горячая линия-Телеком, 2014. — 130 с.: ил. — (Вопросы управления информационной безопасностью. Выпуск 2).

Дополнительная литература:

3. Аверченков В.И. Аудит информационной безопасности : учеб. пособие для вузов. — М. : ФЛИНТА, 2011 — 269 с.

4. Аверченков В. И. Аудит информационной безопасности органов исполнительной власти : учеб. пособие / В. И Аверченков, М.Ю. Рытов, А.В. Кувылкин, М.В. Рудановский. — М. : ФЛИНТА, 2011. — 100 с. — Электронный ресурс. Режим доступа : http://mybrary.ru/users/personal/read/ audit-informatsionnoy-bezopasnosti-organov-ispolnitelnoy-vlasti-3-izdanie/.

5. Астахов А.М. Искусство управления информационными рисками — М. : ДМК Пресс, 2010. — 312 с. — Электронный ресурс. Режим доступа : http://mybrary.ru/users/personal/read/iskusstvo-upravleniya-informatsio-nnyimi-riskami/.

6. Галатенко В.А. Стандарты информационной безопасности : учебное пособие. — 2-е издание / под редакцией академика РАН В.Б. Бетелина. — М. : ИНТУИТ.РУ «Интернет-университет Информационных технологий», 2006. — 264 с.

7. Курило А.П. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиров, В.Б. Голованов и др. — М. : БДЦ-пресс, 2006.–304 с. — Электронный ресурс. Режим доступа : http://padaread.com/?book= 15183&pg=1

8. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. — М. : Горячая линия-телеком, 2001г. — 148 с. — Электронный ресурс. Режим доступа : http://bookre.org/reader?file=550028&pg=1

9. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. — М. : ДМК Пресс, 2004. — 384 с. — Электронный ресурс. Режим доступа : http://mybrary.ru/users/personal/read/upravlenie-informatsionnyimi-riskami-ekonomicheski-opravdannaya-bezopasnost/.

б) нормативные правовые акты и стандарты

Документы - Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Банк данных угроз безопасности информации - Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

[Библиографические описания бумажных ресурсов из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 с указанием имеющегося количества экземпляров (в ЗНБ и/или на кафедре или ином подразделении УрФУ) – суммарное количество экземпляров должно быть ***не менее 0,25 экземпляра*** *каждого из изданий, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику]*

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

[*список с указанием наименования баз данных, информационно-справочных и поисковых систем*]

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.
- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.

ПРОГРАММА МОДУЛЯ

Технические средства и методы защиты информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Техническая защита информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Лучинин Александр Сергеевич	К.т.н., доцент	Доцент	*Учебно-научный центр «Информационная безопасность»*

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

Техническая защита информации

2.1. Технологии обучения, используемые при изучении дисциплины модуля

– Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Концепция технической защиты информации	Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
2	Теоретические основы технической защиты информации	Информации как предмет защиты. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения. Организованные каналы утечки (съема) информации –закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала.
3	Методы и технические	Методы обнаружения каналов утечки по ПЭМИН и через

	средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	закладные устройства. Физические процессы при подавлении опасных сигналов. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Средства предотвращения утечки информации по техническим каналам. Средства 7маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.
4	Организационные основы технической защиты информации	Государственная система защиты информации.Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление проектами в области информационной безопасности

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

1. *Бузов Г.А., Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев .—М. : Горячая линия -Телеком, 2005 .—416 с.*
2. *Домарев В. В. Безопасность информационных технологий. Системный подход: другое. ТИД ДС, 2004. —992 с.*
3. *Технические средства и методы защиты информации. Учебное пособие для вузов/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников, А.А. Солдатов, С.В.Скрыль. Под ред. А.П. Зайцева и А.А. Шелупанова. –4-е изд., испр. и доп. –М.: Горячая линия-Телеком, 2009. –616 с..*
4. *Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности / А. А. Торокин .—Москва : Гелиос АРВ, 2005 .—960 с.*

5. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки: учебник. РГГУ, 2002.—400 с.

6. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности 230201 "Информ. системы и технол." / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .— Москва : Академия, 2006 .—336 с.

5.1.2. Дополнительная литература

1. Зегжда Д. П. Основы безопасности информационных систем: монография. Горячая линия-Телеком, 2000.-452 с.

2. Андрианов, В. И. Устройства для защиты объектов и информации : Справ. пособие / В.И. Андрианов, А.В. Соколов; Под ред. С.А. Золотарева .—2-е изд., перераб. и доп. —СПб.; М. : Полигон : АСТ, 2000 .—256 с.

3. Андрианов В. И.; Золотарев С. А., Соколов А. В. Устройства для защиты объектов и информации: Полигон : АСТ, 2000. (1 экз. в фонде).

4. Барсуков, В. С. Современные технологии безопасности: интегральный подход / В.С. Барсуков, В.В. Водолазкий .—М. : Нолидж, 2000 .—496 с.

5. Горохов П. К. Информационная безопасность Радио и связь, 1995..—224 с.

6. Петраков, А.В.Основы практической защиты информации : Учеб. пособие для вузов по спец. 20. 18. 00 "Защищенные системы связи" / А.В. Петраков .—2-е изд. —М. : Радио и связь, 2000 .—368 с.

Профессиональные базы данных, информационно-справочные системы

Не предусмотрено

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

- *http://www.intuit.ru/ -Национальный открытый университет «ИНТУИТ»,*
- *http://www.edu.ru/ -Федеральный портал. Российское образование,*
- *http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ*
- *http://rtf.ustu.ru -официальный сайт ИРИТ-РтФ.*

2.4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Управление проектами в области информационной безопасности

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.*	*1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet*

		4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	*Information Services 6.0.* *4. Программное обеспечение Microsoft Office версии не менее 2010.*

ПРОГРАММА МОДУЛЯ

Технические средства и методы защиты информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 3

Технические каналы утечки информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Лучинин Александр Сергеевич	К.т.н., доцент	Доцент	*Учебно-научный центр «Информационная безопасность»*

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 3

Технические каналы утечки информации

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Концепция технической защиты информации	Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
2	Теоретические основы технической защиты информации	Информации как предмет защиты. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения. Организованные каналы утечки (съема) информации –закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала.
3	Методы и технические	Методы обнаружения каналов утечки по ПЭМИН и через

	средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	закладные устройства. Физические процессы при подавлении опасных сигналов. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Средства предотвращения утечки информации по техническим каналам. Средства 7маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.
4	Организационные основы технической защиты информации	Государственная система защиты информации.Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление проектами в области информационной безопасности

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

7. Бузов Г.А., Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев .—М. : Горячая линия -Телеком, 2005 .—416 с.

8. Домарев В. В. Безопасность информационных технологий. Системный подход: другое. ТИД ДС, 2004. —992 с.

9. Технические средства и методы защиты информации. Учебное пособие для вузов/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников, А.А. Солдатов, С.В.Скрыль. Под ред. А.П. Зайцева и А.А. Шелупанова. –4-е изд., испр. и доп. –М.: Горячая линия-Телеком, 2009. –616 с..

10. Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности / А. А. Торокин .—Москва : Гелиос АРВ, 2005 .—960 с.

11. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки: учебник. РГГУ, 2002.—400 с.

12. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности 230201 "Информ. системы и технол." / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .— Москва : Академия, 2006 .—336 с.

5.1.2. Дополнительная литература

1. Зегжда Д. П. Основы безопасности информационных систем: монография. Горячая линия-Телеком, 2000.-452 с.

2. Андрианов, В. И. Устройства для защиты объектов и информации : Справ. пособие / В.И. Андрианов, А.В. Соколов; Под ред. С.А. Золотарева .—2-е изд., перераб. и доп. —СПб.; М. : Полигон : АСТ, 2000 .—256 с.

3. Андрианов В. И.; Золотарев С. А., Соколов А. В. Устройства для защиты объектов и информации: Полигон : АСТ, 2000. (1 экз. в фонде).

4. Барсуков, В. С. Современные технологии безопасности: интегральный подход / В.С. Барсуков, В.В. Водолазкий .—М. : Нолидж, 2000 .—496 с.

5. Горохов П. К. Информационная безопасность Радио и связь, 1995..—224 с.

6. Петраков, А.В.Основы практической защиты информации : Учеб. пособие для вузов по спец. 20. 18. 00 "Защищенные системы связи" / А.В. Петраков .—2-е изд. —М. : Радио и связь, 2000 .—368 с.

Профессиональные базы данных, информационно-справочные системы

Не предусмотрено

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

- *http://www.intuit.ru/ -Национальный открытый университет «ИНТУИТ»,*
- *http://www.edu.ru/ -Федеральный портал. Российское образование,*
- *http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ*
- *http://rtf.ustu.ru -официальный сайт ИРИТ-РтФ.*

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Управление проектами в области информационной безопасности

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.*	*1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet*

		4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	*Information Services 6.0.* *4. Программное обеспечение Microsoft Office версии не менее 2010.*

ПРОГРАММА МОДУЛЯ

Технические средства и методы защиты информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 4

Технические средства охраны

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Лучинин Александр Сергеевич	К.т.н., доцент	Доцент	*Учебно-научный центр «Информационная безопасность»*

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 4

Технические средства охраны

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология *(ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);*

2.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Концепция технической защиты информации	Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
2	Теоретические основы технической защиты информации	Информации как предмет защиты. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения. Организованные каналы утечки (съема) информации –закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала.
3	Методы и технические	Методы обнаружения каналов утечки по ПЭМИН и через

	средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	закладные устройства. Физические процессы при подавлении опасных сигналов. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Средства предотвращения утечки информации по техническим каналам. Средства 7маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.
4	Организационные основы технической защиты информации	Государственная система защиты информации.Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление проектами в области информационной безопасности

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

13. Бузов Г.А., Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев .—М. : Горячая линия -Телеком, 2005 .—416 с.

14. Домарев В. В. Безопасность информационных технологий. Системный подход: другое. ТИД ДС, 2004. —992 с.

15. Технические средства и методы защиты информации. Учебное пособие для вузов/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников, А.А. Солдатов, С.В.Скрыль. Под ред. А.П. Зайцева и А.А. Шелупанова. –4-е изд., испр. и доп. –М.: Горячая линия-Телеком, 2009. –616 с..

16. Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности / А. А. Торокин .—Москва : Гелиос АРВ, 2005 .—960 с.

17. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки: учебник. РГГУ, 2002.—400 с.

18. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности 230201 "Информ. системы и технол." / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .— Москва : Академия, 2006 .—336 с.

5.1.2. Дополнительная литература

1. Зегжда Д. П. Основы безопасности информационных систем: монография. Горячая линия-Телеком, 2000.-452 с.

2. Андрианов, В. И. Устройства для защиты объектов и информации : Справ. пособие / В.И. Андрианов, А.В. Соколов; Под ред. С.А. Золотарева .—2-е изд., перераб. и доп. —СПб.; М. : Полигон : АСТ, 2000 .—256 с.

3. Андрианов В. И.; Золотарев С. А., Соколов А. В. Устройства для защиты объектов и информации: Полигон : АСТ, 2000. (1 экз. в фонде).

4. Барсуков, В. С. Современные технологии безопасности: интегральный подход / В.С. Барсуков, В.В. Водолазкий .—М. : Нолидж, 2000 .—496 с.

5. Горохов П. К. Информационная безопасность Радио и связь, 1995..—224 с.

6. Петраков, А.В.Основы практической защиты информации : Учеб. пособие для вузов по спец. 20. 18. 00 "Защищенные системы связи" / А.В. Петраков .—2-е изд. —М. : Радио и связь, 2000 .—368 с.

Профессиональные базы данных, информационно-справочные системы

Не предусмотрено

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

- *http://www.intuit.ru/ -Национальный открытый университет «ИНТУИТ»,*
- *http://www.edu.ru/ -Федеральный портал. Российское образование,*
- *http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ*
- *http://rtf.ustu.ru -официальный сайт ИРИТ-РтФ.*

2.6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Управление проектами в области информационной безопасности

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.*	*1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise;* *2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise;* *3. Microsoft Internet*

		4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	*Information Services 6.0.* *4. Программное обеспечение Microsoft Office версии не менее 2010.*