МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Варлатая С.К.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности
(название кафедры)

_____ Добржинский Ю.В.
(подпись) (Ф.И.О.)

«15» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Техническая защита информации

Направление 10.03.01 Информационная безопасность
(Комплексная защита объектов информатизации)
Форма подготовки очная

курс 4 семестр 8
лекции 36 час.
практические занятия 18 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 90 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект 8 семестр
зачет не предусмотрен
экзамен 8 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от «15» июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., с.н.с., к.т.н.
Составитель: Полянский Д.А., доцент, к.ф-м.н.

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины «Техническая защита информации»

Целью дисциплины является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

Общая трудоемкость освоения дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические работы (18 час.), лабораторные работы (36 час.), самостоятельная работа студентов (54 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен.

Задачами дисциплины являются:

-ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

-ознакомление с техническими каналами утечки акустической (речевой) информации;

-изучение способов и средств защиты информации, обрабатываемой техническими средствами;

-изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;

-изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;

-обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции.

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-7способностью	Знает	возможные нестандартные ситуации

определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Умеет	принимать решения и нести ответственность
	Владеет	навыками и умениями принимать решения в нестандартных ситуациях
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знает	вероятные угрозы и уровни развития технологий защиты информации
	Умеет	организовывать и поддерживать выполнение комплекса мер по информационной безопасности
	Владеет	навыками управления процессом защиты с учетом решаемых задач и организационной структуры объекта защиты
ПК-8 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знает	основы информационной безопасности
	Умеет	принимать участие в эксплуатации подсистем управления информационной безопасностью
	Владеет	навыками применения мер по защите информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Техническая защита информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Каналы утечки информации (20 час.)

Раздел 1. Технические каналы утечки информации. Основные показатели технических средств **(12 час.)**

Тема 1. Основные понятия и определения **(4 час.)**

Тема 2. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами **(4 час.)**

Тема 3. Технические каналы утечки акустической (речевой) информации. **(4 час.)**

Раздел 2. Способы и средства защиты информации от утечки по техническим каналам **(8 час.)**

Тема 1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами **(8 час.)**

МОДУЛЬ 2. Техническая защита информации (16 час.)

Раздел 1. Методы и средства контроля эффективности технической защиты информации **(16 час.)**

Тема 1. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами **(6 час.)**

Тема 2. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам **(6 час.)**

Тема 3. Методы и средства выявления электронных устройств негласного получения информации **(4 час.)**

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (36 час.)

Лабораторная работа №1. Микрофонный эффект в основных и вспомогательных технических средствах **(5 час.)**

Лабораторная работа №2. Устройства несанкционированного съема акустической информации **(6 час.)**

Лабораторная работа №3. Методы и средства съема информации с телефонных линий **(5 час.)**

Лабораторная работа №4. Побочные электромагнитные излучения средств вычислительной техники **(5 час.)**

Лабораторная работа №5. Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях **(5 час.)**

Лабораторная работа №6. Выявление информативных частот ПЭМИН ПК **(5 час.)**

Лабораторная работа №7. Выделение речевого сигнала на фоне шумов и помех **(5 час.)**

Практические занятия (18 час.)

Занятие № 1. Основные характеристики систем радиолокационного наблюдения **(3 час.)**

Занятие № 2. Особенности измерительных радиоприемников **(3 час.)**

Занятие № 3. Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением **(3 час.)**

Занятие № 4. Пассивные и активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях **(3 час.)**

Занятие № 5. Оценка защищенности выделенного помещения от утечки информации по акустическому и виброакустическому каналам. **(3 час.)**

Занятие № 6. Оценка защищенности выделенного помещения от утечки информации по каналам акустоэлектрических преобразований во вспомогательных технических средствах **(3 час.)**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Техническая защита информации» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Каналы утечки информации	ОПК-7 ПК-3 ПК-8	Знает	ПР-1	1-10
			Умеет	ПР-1	1-10
			Владеет	ПР-1	1-10
2	МОДУЛЬ 2. Техническая защита информации	ОПК-7 ПК-3 ПК-7	Знает	ПР-4	11-26
			Умеет	ПР-4	11-26
			Владеет	ПР-4	11-26

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс]: справочник / Г.А. Бузов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2015. — 586 с. — Режим доступа: https://e.lanbook.com/book/94625#book_name

2. Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие / А.А. Титов. — Электрон. дан. — Москва : ТУСУР, 2010. — 197 с. — Режим доступа: https://e.lanbook.com/book/4959#authors

3. Титов, А.А. Технические средства защиты информации [Электронный ресурс] : учебное пособие / А.А. Титов. — Электрон. дан. — Москва : ТУСУР, 2010. — 194 с. — Режим доступа: https://e.lanbook.com/book/4960#authors

Дополнительная литература

1. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/reader/book/1122/#1

2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: https://e.lanbook.com/reader/book/39990/#1

3. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/reader/book/3032/#1

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от

р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020. 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 547, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного,	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно.

практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 412 / D 542, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до проведения семинарского занятия. Работу с теоретическим материалом по теме с использованием учебника или конспекта лекций можно проводить по следующей схеме:

- название темы;
- цели и задачи изучения темы;
- основные вопросы темы;
- характеристика основных понятий и определений, необходимых для усвоения данной темы;
- список рекомендуемой литературы;

– наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т.п.;

– краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

В ходе работы над теоретическим материалом достигается:

– понимание понятийного аппарата рассматриваемой темы;

– воспроизведение фактического материала;

– раскрытие причинно-следственных, временных и других связей;

– обобщение и систематизация знаний по теме.

При подготовке к экзамену рекомендуется проработать вопросы, рассмотренные на лекционных и практических занятиях и представленные в рабочей программе, используя основную литературу, дополнительную литературу и интернет-ресурсы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17"" Aser-173 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 Доска аудиторная
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk

класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	WTL 1810 Мультимедийная аудитория: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 Доска аудиторная
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 547, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 26) Оборудование: "Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718" Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 412 / D 542, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 90) Оборудование: "Мультимедийное оборудование: Экран проекционный Projecta Elpro Large Electron, 500x316 см, размер рабочей области 490x306 Документ-камера Avervision CP 355 AF Мультимедийный проектор Panasonic PT-DZ11OXE, 10 600 ANSI Lumen, 1920x1200 Сетевая видеокамера Multipix MP-HD718 ЖК-панель 47"", Full HD, LG M4716 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA " Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

Приложение 1 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Техническая защита информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	5 неделя	Способы и средства защиты информации от утечки по техническим каналам	54	УО-1
2	12 неделя	экзамен	36	УО-1

Самостоятельная работа студентов включает:

– освоение лекционного материала;

– выполнение индивидуального домашнего задания;

– оформление выполненного индивидуального домашнего задания;

– подготовку к защите выполненного индивидуального домашнего задания.

Приложение 2 к рабочей программе учебной дисциплины

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Техническая защита информации»
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль подготовки - «Комплексная защита объектов информатизации»
Форма подготовки - очная

Владивосток
2019

Обучающиеся должны выполнять индивидуальные задания. Задания должны быть выполнены в процессе изучения соответствующего раздела курса. При выполнении заданий возможно использование учебно-методической литературы и электронных лекций курса.

Перечень типовых экзаменационных вопросов.

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации

2. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).

3. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.

4. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.

5. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.

6. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.

7. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата). Дальность перехвата речевого сигнала средством акустической разведки направленными микрофонами.

8. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.

9. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

10. Экранирующие материалы, их основные характеристики. Формула для расчета коэффициента экранирования для электрической и магнитной

составляющей электромагнитного поля. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).

11. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.

12. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации. Основные требования по установке системы пространственного зашумления на объекте информатизации. Основные характеристики генераторов шума.

13. Основные требования к системе электропитания технических средств. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет наводок побочных электромагнитных излучений. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств. Основные характеристики фильтров нижних частот (ФНЧ). Схемы установки помехоподавляющих фильтров на объекте информатизации.

14. Характеристики речевого сигнала. Разборчивость речи.

15. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

16. Средства звуко- и виброизоляции выделенных помещений. Звукоизолирующие кабины. Специальные защищенные помещения.

17. Порядок проведения контроля эффективности защиты ВТСС. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.

18. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

19. Сканирующие приемники (принцип работы, основные характеристики). Этапы выявления РЗ. Методы обнаружения, идентификации РЗ и определения их местоположения.

20. Порядок организации защиты информации на объектах информатизации.

21. Предварительное специальное обследование объекта информатизации.

22. Аналитическое обоснование необходимости создания СТЗИ объекта (содержание, порядок проведения).

23. Замысел создания СТЗИ. Техническое задание на разработку СТЗИ объекта информатизации.

24. Организация аттестации объекта информатизации по требованиям безопасности информации. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.

25. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.

26. Заключение по результатам аттестационной проверки объекта информатизации. Аттестат соответствия объекта информатизации.

ТЕМАТИКА И ПЕРЕЧЕНЬ КУРСОВЫХ РАБОТ И РЕФЕРАТОВ

Темы курсовых работ:

1. Демаскирующие признаки объектов защиты.
2. Источники и носители конфиденциальной информации.
3. Источники опасных сигналов.
4. Виды угроз безопасности информации.
5. Способы и средства добывания информации техническими средствами.

6. Технические каналы утечки информации (реальные и потенциальные).

7. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде. Принципы физического и химического анализа веществ.

8. Способы и средства инженерной технической защиты.

9. Модели злоумышленников. Уровни физической безопасности объектов. Типовая структура системы физической безопасности объекта.

10. Системы автономной и централизованной охраны.

11. Способы и средства идентификации людей.

12. Способы и средства видеоконтроля. Структура системы видеоконтроля.

13. Способы и средства нейтрализации угроз. Виды способов и средств нейтрализации угроз.

14. Средства управления системой инженерно-технической защиты.

15. Автоматизированные интегральные системы охраны объектов, их структура и тенденция развития.

16. Способы и средства защиты информации от наблюдения.

17. Способы и средства противодействия наблюдению в оптическом диапазоне волн.

18. Способы и средства противодействия радиолокационному и гидроакустическому наблюдению.

19. Способы информационного скрытия объектов от радиолокационного наблюдения.

20. Средства дезинформирования и пассивного зашумления изображения на экране радиолокатора.

21. Виды радиопоглощающих покрытий. Способы активного подавления сигналов радиолокаторов.

22. Способы и средства защиты информации от подслушивания.

23. Способы и средства информационного скрытия акустических сигналов и речевой информации.

24. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки

25. Организационные и технические меры по инженерно-технической защите информации в организации.

26. Средства подавления сигналов закладных устройств в телефонных линиях и цепях электропитания.

27. Функции сотрудников службы безопасности, обеспечивающие инженерно-техническую защиту информации.

28. Сущность технического контроля эффективности защиты информации.

29. Моделирование объекта защиты.

30. Моделирование угроз информации.

31. Инженерно-техническое обеспечение безопасности информации путём осуществления необходимых организационно технических мероприятий.