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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Техническая защита информации
Специальность 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

курс 5 семестр 9
лекции 36 час.
практические занятия 00 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 9 / пр. 0 / лаб. 9 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 18 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 9 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

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

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель: Власов А.А.

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)

ABSTRACT

Specialist's degree in *10.05.01 Computer Security*

Specialization "*Mathematical Methods for Information Security*"

Course title: *Technical information protection*

Basic part of Block 1, _4_credits

Instructor: *Polyansky D.A.*

At the beginning of the course a student should be able to:

• ability to apply research methods in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);

• ability to use regulatory legal acts in their professional activities (OPK-5);

Learning outcomes:

- OPK-9 - the ability to develop formal models of security policies, access control policies and information flows in computer systems, taking into account information security threats
- PC-19 - the ability to perform technical checks and preventive inspections of technical means of information protection

Course description: The course of lectures is based on a step-by-step narration from technical channels of information leakage and means of technical protection of information.

Main course literature:

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

Form of final control: *exam.*

Аннотация к рабочей программе дисциплины
«Техническая защита информации»

Курс учебной дисциплины «Техническая защита информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.12.03.

Общая трудоемкость освоения дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (36 час.), самостоятельная работа (36 час., в том числе 36 час. на подготовку к экзамену). Дисциплина реализуется на 5 курсе, в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Техническая защита информации» логически и содержательно связана с такими курсами, как «Операционные системы», «Основы информационной безопасности», «Аппаратные средства вычислительной техники».

Курс лекций построен на пошаговом повествовании от технических каналов утечки информации и средствам технической защиты информации.

Цель дисциплины: раскрыть природу формирования технических каналов утечки информации, сформировать представление о проблемах защиты технических каналов утечки информации, выработать умения и навыки по определению потенциальных каналов утечки информации на объектах информатизации, по выработке рекомендаций по защите конкретного канала утечки, ознакомить с процессом сертификации средств защиты и мероприятиями аттестации объектов информатизации на соответствие требованиям безопасности информации.

Задачи дисциплины:

- привести анализ физических процессов приводящих к появлению опасных сигналов демаскирующих защищаемые объекты;

- дать физические основы процессов образования технических каналов утечки информации;

- дать физическое обоснование технических характеристик каналов утечки информации;

- изложить концепцию и методы инженерно-технической защиты информации;

- дать представление о формировании базы нормативных документов по противодействию технической и видам контроля эффективности защиты информации.

Для успешного изучения дисциплины «Техническая защита информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-9 – способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Уметь	разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеть	навыками разработки моделей угроз и моделей нарушителя

ПК-19 – способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать	принципы работы оборудования по защите информации
	Уметь	проводить проверку технического состояния оборудования по защите информации
	Владеть	навыками настройки оборудования 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

Раздел I. Технические каналы утечки информации (18 час.)

Тема 1. Физические основы функционирования систем обработки и передачи информации (2 час.)

1.1. Информация; обработка и передача информации;

1.2. Физические принципы обработки, передачи и хранения информации.

Тема 2. Принципы и способы добывания информации (2 час.)

2.1. Основными принципами добывания информации:

2.2. Способы добывания информации;

2.3. Методы синтеза информации.

Тема 3. Акустический канал утечки информации (4 час.)

3.1. Виды акустических каналов;

3.2. Основные характеристики акустических сигналов речи;

3.3. Способы перехвата по акустическому каналу.

Тема 4. Вибрационный канал утечки информации (2 час.)

4.1. Среда распространения сигнала;

4.2. Основные характеристики вибрационных каналов; виброакустические

каналы;

4.3. Способы перехвата сигнала.

Тема 5. Электромагнитный канал утечки информации (6 час.)

5.1. Переносчики информации; среда распространения сигнала;

5.2. Классификация электромагнитных каналов утечки информации.

Тема 6. Оптический канал утечки информации (2 час.)

6.1. Среды распространения информации; их виды и свойства;

6.2. Носители информации.

Раздел II. Средства технической защиты (18 час.)

Тема 7. Приборы виброакустической защиты (4 час.)

7.1. Способы защиты от утечек информации по виброакустическому каналу;

7.2. Комплекс программных и аппаратных мер для предотвращения утечек информации.

Тема 8. Нелинейная локация (2 час.)

8.1. Теоретические основы нелинейной локации;

8.2. Применение нелинейной локации;

8.3. Ложные срабатывания ЛН.

Тема 9. Средства защиты проводных линий (4 час.)

9.1. Методы противодействия снятию информации с проводных линий;

9.2. Защитные устройства;

9.3. Классификация защитных устройств; принципы их работы;

Тема 10. Средства выявления радиосигналов закладных устройств (4 час.)

10.1. Способы обнаружения закладных устройств;

10.2. Методы активной борьбы с закладными устройствами.

Тема 11. Пеленгация и подавление нежелательных сигналов (2 час.)

11.1. Способы отделения нежелательных сигналов от полезных;

11.2. Методы подавления нежелательных сигналов.

Тема 12. Выявление устройств записи информации (2 час.)

12.1. Способы выявления устройств записи информации;

12.2. Средства защиты.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (36 час.)

Лабораторная работа № 1. Определение потенциальных технических каналов утечки информации по исходным данным для объекта информатизации (4 час.)

Лабораторная работа № 2. Возможности специальных исследований по защите объекта информатизации от утечки акустической информации «Звезда», «Спрут-7А» (6 час.)

Лабораторная работа № 3. Организация защиты выделенного помещения от утечки речевой акустической информации по ТКУИ (4 час.)

Лабораторная работа № 4. Возможности специальных исследований по защите объекта информатизации от утечки по каналу ПЭМИН «Заря», «Навигатор-7П» (4 час.)

Лабораторная работа № 5. Возможность выявления каналов утечки информации нелинейным локатором NR-900EM (4 час.)

Лабораторная работа № 6. Специальные исследования ПЭВМ с использованием измерительных приемников (4 час.)

Лабораторная работа № 7. Методика оценки защищенности информации, обрабатываемой ТСПИ, от утечки за счет наводок на вспомогательные средства и системы (6 час.)

Лабораторная работа №8. Возможности по защите информации генераторов пространственного и линейного зашумления "Гром-ЗИ4", "Гром-ЗИ6" (4 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	Раздел |I. Технические каналы утечки информации	ОПК-7 ОПК-9, ПК-19	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-17
			умеет	лабораторные работы (ПР-6)	1-17
			владеет	конспект (ПР-7),	1-17
2	Раздел II. Средства технической защиты	ОПК-7 ОПК-9, ПК-19	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	18-56
			умеет	лабораторные работы (ПР-6)	18-56
			владеет	конспект (ПР-7),	18-56

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) 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. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Техническая защита информации: Лабораторный практикум / Под редакцией Ю.Ф. Каторина - СПб: НИУ ИТМО, 2013. - 112 с. http://www.iprbookshop.ru/68715.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Лекция 9. Технические средства защиты информации [Электронный ресурс]. - Электрон. дан. — Режим доступа: https://studfiles.net/preview/6212231/page:20/

2. Лекция 4. Инженерно-техническая защита информации [Электронный ресурс]. - Электрон. дан. — Режим доступа: https://studfiles.net/preview/5157335/page:3/

3. Усков. Лекции по информационной безопасности [Электронный ресурс]. - Электрон. дан. — Режим доступа: http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/

Перечень информационных технологий и программного обеспечения.

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Специализированная лаборатория кафедры ИБ. 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.
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.

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 743, 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

Количество аудиторных часов, отведенных на изучение дисциплины «Техническая защита информации», составляет 72 часа. На самостоятельную работу – 36 часа (в том числе на подготовку к экзамену – 18 часов). При этом аудиторная нагрузка состоит из 36 лекционных часов и 36 часов лабораторных занятий.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к лабораторным занятиям предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Специализированная лаборатория кафедры ИБ. 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 – 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 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: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk 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 743, 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 – 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.

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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»
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
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	1-18 недели обучения	Подготовка лабораторных работ (выполнение отчета по лабораторным работам 1-8)	36	Отчет о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

Рекомендации по самостоятельной работе студентов

1. Применение направленных микрофонов и методы противодействия.
2. Применение лазерных микрофонов и методы противодействия.
3. Приборы ВАЗ и области из применения.
4. Фонемный клонер.
5. Генераторы линейного зашумления.
6. Генераторы пространственного зашумления.
7. Выявление случайных антенн.
8. Техническая защита электрических сетей.
9. Техническая защита телефонных и компьютерных сетей.
10. Определение акустоэлектрических преобразований.

Подготовка отчета к лабораторным работам предполагает повторение лекционного материала и выполнение практического задания 1 из Раздела II РПУД. В результате студент должен предоставить отчет о проделанной работе.

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

Приложение 2

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Техническая защита информации»
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-9 – способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Уметь	разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеть	навыками разработки моделей угроз и моделей нарушителя
ПК-19 – способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать	принципы работы оборудования по защите информации
	Уметь	проводить проверку технического состояния оборудования по защите информации
	Владеть	навыками настройки оборудования по защите информации

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел |I. Технические каналы утечки информации	ОПК-7 ОПК-9, ПК-19	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-17
			умеет	лабораторные работы (ПР-6)	1-17
			владеет	конспект (ПР-7),	1-17
2	Раздел II. Средства технической защиты	ОПК-7 ОПК-9, ПК-19	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	18-56
			умеет	лабораторные работы (ПР-6)	18-56

владеет конспект (ПР-7), 18-56

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине в 9 семестре – экзамен.

Для допуска к экзамену в 9 семестре необходимо сдать все лабораторные работы. В случае, если ко дню проведения экзамена обучающийся не сдал какие-либо из лабораторных работ, он получает возможность сдать их на консультации перед экзаменом. В 9 семестре экзамен выставляется на основании сдачи всех лабораторных работ и сдачи экзаменационного билета. Для подготовки к ответу на экзамене обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

Для получения «зачтено» ответ студента должен соответствовать следующим минимальным требованиям: полный ответ на 1 вопрос или частичный ответ на 2 вопроса; допускаются нарушения в последовательности изложения; демонстрируются поверхностные знания вопроса; имеются затруднения с выводами; допускаются нарушения норм литературной речи.

Оценка «не зачтено» выставляется в случае если: обучающийся не ответил полно ни на один вопрос; материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине; имеются заметные нарушения норм литературной речи.

Оценочные средства для промежуточной аттестации
Список вопросов к экзамену

1. Способы защиты информации. Разновидности инженерно-технических способов защиты.
2. Что такое технический канал утечки информации. Какие физические каналы он включает.
3. Что такое преобразователи. Побочная система связи.
4. Параметры преобразователя. Основные источники образования технических каналов утечки.
5. Типы каналов утечки информации. Разновидности акустических, электромагнитных и электронных каналов.
6. Акустические каналы утечки.
7. Разновидности и принцип действия направленных микрофонов.
8. Системы лазерного прослушивания.
9. Принцип ВЧ-навязывания. Способы защиты от ВЧ-навязывания.
10. Способы защиты информации от утечки по акустическому каналу. Системы ультразвукового подавления.
11. Системы акустической маскировки. Типы зашумления, фонемный клонер. Основные критерии эффективности СВЗ.
12. Системы подавления диктофонов путем воздействия на электронные цепи звукозаписывающего устройства.
13. Фурье-разложение. Полоса пропускания и влияние на неё уровня шума.
14. Приборы обнаружения технических средств перехвата информации. Принцип действия нелинейного локатора и кабельного радара.
15. Устройства, фиксирующие электромагнитное излучение технических средств перехвата информации.
16. Принцип действия сканера, частотомера и анализатора спектра.
17. Детектор инфракрасного излучения. Селективный вольтметр.
18. Электромагнитный канал утечки информации. Принцип работы DECT телефонов и методы перехвата информации, передаваемой через них.
19. Маскиратор речи и скремблер. Разновидности скремблирования.
20. Методы и средства защиты телефонных линий.
21. Телефонное ухо.
22. Радиозакладки. Схема устройства. Что такое телефонный жук.
23. Обобщенные данные радиозакладок, применяемых в Р.Ф. Характеристики закладок.
24. Варианты питания радиозакладок.

25. Чем обеспечивается скрытность радиозакладок. Частотные диапазоны работы.
26. Нестабилизированные и стабилизированные закладки. Способы стабилизации.
27. Пассивные радиозакладки
28. Приёмники информации с радиозакладок
29. Специальные комплексы из передатчика и приёмника и их характеристики
30. Индикаторы поля. Что такое аттенюатор.
31. Дифференциальный индикатор поля.
32. Панорамные приёмники (сканеры). Режимы работы.
33. Последовательный сканер.
34. Параллельный сканер.
35. Анализаторы спектра (спектральные корреляторы) и их функции.
36. Состав спектрального коррелятора.
37. Комплексы, сформированные на базе серийного сканера и их функции.
38. Нелинейные локаторы. Физические основы работы.
39. Характеристики нелинейных локаторов.
40. Непрерывный и импульсный локатор.
41. Способы селекции помех от случайных источников
42. Этапы поиска устройств негласного съёма информации. Расписать подготовительный этап.
43. Этапы поиска устройств негласного съёма информации. Расписать физический поиск и визуальный осмотр.
44. Алгоритм поиска радиозакладных устройств. Что такое опорная панорама.
45. Выявление технических средств, сливающих информацию по токоведущим линиям.
46. Что такое антенна. Особенности работы в режиме приёма и передачи.
47. Диаграмма направленности, коэфф.усиления, коэф.направленного действия.
48. Дальняя, ближняя и средняя зона антенны.
49. Фазированная антенная решётка.
50. Кольцевая антенна. Расчёт эффективной высоты. Сопротивление излучения. Ферритная антенна.
51. Информационное и энергетическое скрытие.
52. Пассивные способы подавления опасных сигналов.

53. Активные способы подавления опасных сигналов.
54. Электростатическое и магнитное экранирование.
55. Электромагнитное экранирование.
56. Линейное зашумление и пространственное зашумление

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.