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 ДИСЦИПЛИНЫ
Защита информации от технической разведки
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 5 семестр 10
лекции 36 час.
практические занятия 18 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 90 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 90 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 10 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: *Protection of information from technical intelligence*
Variable part of Block 1, _5_credits
Instructor: *Polyansky D.A.*
At the beginning of the course a student should be able to:

• ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2) when solving professional problems;

• the ability to understand the importance of information in the development of modern society, to apply the achievements of information technologies to search and process information on the profile of activities in global computer networks, library collections and other sources of information (OPK-3);

• the ability to take into account modern trends in the development of computer science and computing technology, computer technology in their professional activities, to work with software tools for general and special purposes (OPK-7);

• the ability to install, adjust, test and maintain modern common and special software, including operating systems, database management systems, network software (PC-17).

Learning outcomes: (PC-12) the ability to carry out instrumental monitoring of the security of computer systems

(PC-14) the ability to organize work on the implementation of information security, including limited access

(PC-20) the ability to perform work on the restoration of the health of information security tools in the event of emergency situations

Course description: The discipline "Protection of Information from Technical Intelligence" provides for the acquisition of knowledge and skills in the field of technical intelligence, as well as ensuring the protection of information from technical intelligence assets. The study of this discipline contributes to the development of methods and means of protection of the identified channels of obtaining information.

Main course literature:

1. Белозерцев Л.Н., Зарипов С.Н., Журавленко Н.И. Противодействие речевой разведке / Л.Н. Белозерцев, С.Н. Зарипов, Н.И. Журавленко – Уфа : Башкирский государственный университет, 2014. – 218 с. — Режим доступа: https://elibrary.ru/item.asp?id=26204058

2. Дождиков В.Г., Салтан М.И. Краткий энциклопедический словарь по информационной безопасности / В.Г. Дождиков, М.И. Салтан – М. : Энергия, 2012. – 240 с. — Режим доступа: https://elibrary.ru/item.asp?id=21557324

3. Перфилов О.Ю., Киселев Д.Н. Радиомониторинг и распознавание

радиоизлучений / О.Ю. Перфилов, Д.Н. Киселев – М. : Горячая линия - Телеком, 2015. – 90 с. — Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204903.html

Form of final control: *exam.*

Аннотация к рабочей программе дисциплины
«Защита информации от технической разведки»

Рабочая программа учебной дисциплины «Защита информации от технической разведки» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин вариативной части учебного плана Б1В.05.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 академических часа. Учебным планом предусмотрены лекционные занятия (36 часов), лабораторные работы (36 часов), практические занятия (18 часов), самостоятельная работа (54 часов). Дисциплина реализуется на 5 курсе, в А семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Защита информации от технической разведки» основана на предварительном изучении следующих дисциплин: «Информатика», «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Аппаратные средства вычислительной техники», «Защита программ и данных». Знания и практические навыки, полученные при изучении дисциплины «Защита информации от технической разведки», обеспечивают освоение следующих дисциплин: «Инженерная защита и охрана объектов», «Программно-аппаратные средства обеспечения информационной безопасности», «Теория и проектирование защищенных систем».

Дисциплина имеет практическую направленность, при этом большое значение для освоения дисциплины имеют лабораторные занятия. В ходе реализации дисциплины в рамках лекционных, лабораторных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов защиты информации от

технической разведки.

Дисциплина «Защита информации от технической разведки» обеспечивает приобретение знаний и умений в области технической разведки, а также обеспечения защиты информации от средств технической разведки. Изучение этой дисциплины способствует освоению способов и средств защиты выявленных каналов добывания информации.

Цель дисциплины – раскрыть природу ведения технической разведки, сформировать представление о проблемах защиты информации от технической разведки, выработать умения и навыки применению средств защиты информации от технической разведки, сформировать умения по выработке рекомендаций по защите от технической разведки.

Задачи:

- изучить основных угроз безопасности информации и модели нарушителя в КС;
- изучить основные этапы и процедуры добывания информации технической разведки;
- освоить методы спектрального анализа с помощью пакета прикладных программ MATLAB;
- изучить методы работы с комплексом выявления технических каналов утечки информации;
- изучить возможность выявления каналов утечки информации нелинейным локатором NR-900EM;
- оценить защищенность информации, обрабатываемой ТСПИ, от утечки по каналу ПЭМИ.

Для успешного изучения дисциплины «Защита информации от технической разведки» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории

вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

•способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

•способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);

•способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17).

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-12) способность проводить инструментальный мониторинг защищенности компьютерных систем	Знает	особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов
	Умеет	анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней
	Владеет	программными и техническими средствами защиты информации в компьютерных системах
(ПК-14) способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знает	организационные, программные и технические методы защиты информации
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям
	Владеет	методами и практическими навыками анализа создания систем защиты информации

(ПК-20) способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знает	методы технической и программной защиты информации
	Умеет	тестировать конкретные компьютерные системы с использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях где они расположены
	Владеет	программными и аппаратными средствами контроля защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информации от технической разведки» 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. Техническая разведка (20 час.)

Тема 1. Классификация технической разведки. Возможности видов технической разведки (4 час.)

1.1 Наземная техническая разведка.

1.2 Воздушная техническая разведка.

1.3 Космическая техническая разведка.

1.4 Морская техническая разведка.

Тема 2. Демаскирующие признаки объектов и источников информации для технических средств разведки (12 час.)

2.1 Признаки, характеризующие физические поля, создаваемые объектом.

2.2 Признаки химических и биологических сред.

2.3 Признаки, характеризующие объект.

2.4 Признаки, характеризующие физические свойства вещества объекта.

2.5 Признаки деятельности защищаемого объекта.

Тема 3. Основные этапы и процедуры добывания информации технической разведки (4 час.)

3.1 Организация добывания информации.

3.2 Добывание данных и сведений.

3.3 Информационная работа.

Раздел II. Средства защиты информации от технической разведки (16 час.)

Тема 1. Задачи систем защиты информации (12 час.)

1.1 Определение защищаемой информации.

1.2 Категорирование защищаемой информации.

1.3 Обеспечение безопасности информации на уровне, соответствующем актуальной политике информационной безопасности.

1.4 Реализация повышенных требований к безопасности информации.

1.5 Нормативно-правовое обеспечение деятельности по защите информации.

1.6 Комплексное и целевое планирование обеспечения информационной безопасности, установление и поддержание установленных режимов безопасности.

Тема 2. Способы и средства защиты выявленных каналов добывания информации технической разведкой (4 час.)

2.1 Способы защиты каналов.

2.2 Средства защиты каналов.

2.3 Классификация методов защиты информации.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 час.)

Занятие 1. Работа с многоканальным комплексом радиоконтроля (10 час.)

1. Оценка защищенности речевой информации.
2. Защита от скрытой звукозаписи посредством диктофона.

Занятие 2. Защита телефонного канала от утечки информации (8 час.)

1. Локация полупроводниковых приборов.
2. Видеонаблюдение.
3. Скремблеры.

Лабораторные работы (36 час.)

Лабораторная работа № 1. Освоение методов спектрального анализа с помощью пакета прикладных программ MATLAB (4 час.)

Лабораторная работа № 2. Изучение методов работы с комплексом выявления технических каналов утечки информации ST 031P («Пиранья») (4 час.)

Лабораторная работа № 3. Настройка совместной работы комплекса выявления технических каналов утечки информации ST 031P («Пиранья») и персонального компьютера и выявление каналов утечки информации с помощью данного программно-аппаратного комплекса (4 час.)

Лабораторная работа № 4. Возможности по защите информации генераторов пространственного и линейного зашумления "Гром-ЗИ4", "Гром-ЗИ6" (4 час.)

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

Лабораторная работа № 6. Проверка возможности утечки речевой информации из помещения и оценка уровня акустической защиты с помощью программно-аппаратного комплекса «Спрут» (4 час.)

Лабораторная работа № 7. Методика оценки защищенности информации, обрабатываемой ТСПИ, от утечки за счет наводок на вспомогательные средства и системы (4 час.)

Лабораторная работа №8. Методика оценки защищенности информации, обрабатываемой ТСПИ, от утечки по каналу ПЭМИ (4 час.)

Лабораторная работа №9. Создание нестабилизированного закладного радиоустройства, выявление сигнала и обнаружение местонахождения (2 час.)

Лабораторная работа №10. Составление опорной схемы кабинета (2 час.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информации от технической разведки» 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. Техническая разведка	ПК-12, ПК-14, ПК-20	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-12
			умеет	лабораторные работы (ПР-6)	1-12
			владеет	конспект (ПР-7),	1-12
2	Раздел II. Средства защиты информации от технической разведки	ПК-12, ПК-14, ПК-20	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	13-21
			умеет	лабораторные работы (ПР-6)	13-21
			владеет	конспект (ПР-7),	13-21

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

(электронные и печатные издания)

1. Белозерцев Л.Н., Зарипов С.Н., Журавленко Н.И. Противодействие речевой разведке / Л.Н. Белозерцев, С.Н. Зарипов, Н.И. Журавленко – Уфа : Башкирский государственный университет, 2014. – 218 с. — Режим доступа: https://elibrary.ru/item.asp?id=26204058
2. Дождиков В.Г., Салтан М.И. Краткий энциклопедический словарь по информационной безопасности / В.Г. Дождиков, М.И. Салтан – М. : Энергия, 2012. – 240 с. — Режим доступа: https://elibrary.ru/item.asp?id=21557324
3. Перфилов О.Ю., Киселев Д.Н. Радиомониторинг и распознавание радиоизлучений / О.Ю. Перфилов, Д.Н. Киселев – М. : Горячая линия - Телеком, 2015. – 90 с. — Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204903.html

Дополнительная литература

(печатные и электронные издания)

1. Ведев А.Л., Хромов М.Ю. Методология построения финансовых балансов секторов экономики / А.Л. Ведев, М.Ю. Хромов – М. : Дело, 2015. – 132 с. — Режим доступа: http://www.studentlibrary.ru/book/ISBN9785774910441.html
2. Рихтер С.Г., Попов О.Б. Цифровая обработка сигналов в трактах звукового вещания / С.Г. Рихтер, О.Б. Попов – М. : Горячая линия - Телеком, 2015. – 342 с. — Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202893.html
3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов – М. : Горячая линия - Телеком, 2015. – 586 с. — Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Защита информации от разведки [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://dic.academic.ru/dic.nsf/emergency/776/защита
2. ГОСТ Р 50922-96 [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://rfcmd.ru/sphider/docs/InfoSec/GOST_R_50922-96.htm
3. Противодействие техническим средствам разведки [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://ru.bmstu.wiki/Противодействие_техническим_средствам_разведки

Перечень информационных технологий
и программного обеспечения

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 734, Компьютерный класс, 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 «Защита информации от технической разведки», составляет 72 часа. На самостоятельную работу – 36 часов.

Аудиторная нагрузка состоит из 18 лекционных часов, 18 часов практических работ и 36 часов лабораторных работ. На лекционных занятиях обучающийся получает теоретические знания, усвоение которых необходимо для дальнейшего выполнения лабораторных и практических работ. Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

Подготовка к лабораторным работам и практическим занятиям предполагает повторение лекционного материала. В результате выполнения работы студент предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы, результаты и выводы о проделанной работе.

В рамках указанной дисциплины итоговой формой аттестации является зачет. Вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях. Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников из списка литературы и материалов по лабораторным и практическим работам.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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 734, Компьютерный класс, 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 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

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 «Защита информации от технической разведки»
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 практических заданий и лабораторных работ (выполнение отчетов к лабораторным и практическим работам)	54	Отчеты о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

Подготовка отчета по лабораторным и практическим работам предполагает повторение лекционного материала и выполнение задания для лабораторных и практических работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на лабораторную или практическую работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к зачету, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД.

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 «Защита информации от технической разведки»
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	Этапы формирования компетенции	
(ПК-12) способность проводить инструментальный мониторинг защищенности компьютерных систем	Знает	особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов
	Умеет	анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней
	Владеет	программными и техническими средствами защиты информации в компьютерных системах
(ПК-14) способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знает	организационные, программные и технические методы защиты информации
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям
	Владеет	методами и практическими навыками анализа создания систем защиты информации
(ПК-20) способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знает	методы технической и программной защиты информации
	Умеет	тестировать конкретные компьютерные системы с использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях где они расположены
	Владеет	программными и аппаратными средствами контроля защиты 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. Техническая разведка	ПК-12, ПК-14, ПК-20	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-12
			умеет	лабораторные работы (ПР-6)	1-12
			владеет	конспект (ПР-7),	1-12
2	Раздел II. Средства	ПК-12,	знает	собеседование	13-21

защиты информации от технической разведки	ПК-14, ПК-20		(ОУ-1), коллоквиум (ОУ-2).	
		умеет	лабораторные работы (ПР-6)	13-21
		владеет	конспект (ПР-7),	13-21

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачет.

Для допуска к зачету обучающийся должен получить оценку «зачтено» по всем лабораторным и практическим работам курса. Критерии оценивания лабораторных и практических работ представлены далее в данном Приложении.

Зачет проводится в форме собеседования (УО-1), вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на зачете обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки учитываются:

-знание основных терминов и понятий курса;

-знание и владение методами и средствами решения задач;

-последовательное изложение материала курса;

-умение формулировать некоторые обобщения по теме вопросов;

-достаточно полные ответы на вопросы;

-умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для промежуточной аттестации

Список вопросов на зачет

1. Наземная техническая разведка.
2. Воздушная техническая разведка.
3. Космическая техническая разведка.
4. Морская техническая разведка.
5. Признаки, характеризующие физические поля, создаваемые объектом.
6. Признаки химических и биологических сред.

7. Признаки, характеризующие объект.

8. Признаки, характеризующие физические свойства вещества объекта.

9. Признаки деятельности защищаемого объекта.

10. Организация добывания информации.

11. Добывание данных и сведений.

12. Информационная работа.

13. Определение защищаемой информации.

14. Категорирование защищаемой информации.

15. Обеспечение безопасности информации на уровне, соответствующем актуальной политике информационной безопасности.

16. Реализация повышенных требований к безопасности информации.

17. Нормативно-правовое обеспечение деятельности по защите информации.

18. Комплексное и целевое планирование обеспечения информационной безопасности, установление и поддержание установленных режимов безопасности.

19. Способы защиты каналов.

20. Средства защиты каналов.

21. Классификация методов защиты информации.

Каждый студент должен ответить на два вопроса из списка выше. Результаты зачета оцениваются по двухбалльной системе («зачтено», «не зачтено») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

-знание основных терминов и понятий курса;

-знание и владение методами и средствами решения задач;

-последовательное изложение материала курса;

-умение формулировать некоторые обобщения по теме вопросов;

-достаточно полные ответы на вопросы;

-умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«зачтено».** Хорошее знание основных терминов и понятий курса. Хорошее знание и владение методами и средствами решения задач. Последовательное изложение материала курса. Умение формулировать некоторые обобщения по теме вопросов. Достаточно полные ответы на вопросы. Умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«не зачтено».** Неудовлетворительное знание основных терминов и понятий курса. Неумение решать задачи. Отсутствие логики и последовательности в изложении материала курса. Неумение формулировать отдельные выводы и обобщения по теме вопросов. Неумение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются лабораторные работы (ПР-6) и 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.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся лабораторные и практические работы. Темы лабораторных и практических работ представлены в Разделе II РПУД. Критерии оценки представлены в таблице:

Оценка	Критерий
Зачтено	Отчёт по лабораторной и практической работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на лабораторную и практическую работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ. Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных

	источников литературы.
Незачтено	Отчёт по лабораторной и практической работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ. Конспект не содержит основных понятий, терминов, положений по данной теме