



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 18 час.
практические занятия 18 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 9 /пр. 00 /лаб. 12 час.
в том числе в электронной форме лек. 00 /пр. 00 /лаб. 00 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 21 час.
в том числе в электронной форме 00 час.
самостоятельная работа 36 час.
в том числе на подготовку к экзамену 00 час.
курсовая работа / курсовой проект не предусмотрены
зачет 10 семестр
экзамен не предусмотрен

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 (ли): Полянский Д.А. к.ф.-м.н., доцент.

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, 3 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:

Discipline is practical, with laboratory classes being of great importance for mastering the discipline. During the implementation of the discipline in the framework of lectures, laboratory and practical classes, methods of active / interactive learning are used that implement a visual representation of the results of information protection from technical intelligence.

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 knowledge control: *pass-fail exam*

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

Рабочая программа учебной дисциплины «Защита информации от технической разведки» разработана для студентов 5 курса по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав обязательных дисциплин вариативной части учебного плана с кодом Б1.В.ОД.5.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 академических часа. Учебным планом предусмотрены лекционные занятия (18 часов), лабораторные работы (36 часов), практические занятия (18 часов), самостоятельная работа (36 часов). Дисциплина реализуется на 5 курсе, в А семестре. Форма контроля по дисциплине – зачет.

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 общекультурные 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	Знает	организационные, программные и технические методы защиты информации.
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным реальным условиям.

доступа	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: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Техническая разведка (10 час.)

Тема 1. Классификация технической разведки. Возможности видов технической разведки (2 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 (6 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 (2 час.)

- 3.1 Организация добывания информации.

3.2 Добывание данных и сведений.

3.3 Информационная работа.

Раздел II. Средства защиты информации от технической разведки (8 час.)

Тема 1. Задачи систем защиты информации (6 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 (2 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,	знает	ПР-7	1-12
		ПК-14,	умеет	ПР-6	1-12
		ПК-20	владеет	ПР-6	1-12
2	Раздел II. Средства защиты информации от технической разведки	ПК-12,	знает	ПР-7	13-21
		ПК-14,	умеет	ПР-6	13-21
		ПК-20	владеет	ПР-6	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

Для выполнения лабораторных и практических работ используется пакет прикладных программ MATLAB. Для работы с литературой из списка необходимо наличие у студента аккаунтов в указанных электронно-библиотечных системах: «eLIBRARY.RU» (<http://elibrary.ru/>), «ЭБС

"Консультант студента"» (<http://www.studentlibrary.ru/>).

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 314, Специализированная лаборатория кафедры ИБ. Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь,
---	--

<p>индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>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 видеочкамера Multipix MP-HD718 " Доска аудиторная</p>
<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 733, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Моноблок lenovo C360G-i34164G500UDK 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 видеочкамера Multipix MP-HD718" Доска аудиторная</p>
<p>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</p>	<p>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</p>

промежуточной аттестации.	White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avergence CP355AF ЖК-панель 47", Full HD, LG M4716 ССВА Мультимедийный проектор Mitsubishi EW330U, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP- HD718 Доска аудиторная
---------------------------	--



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»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «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	1-17 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	18	Отчет о выполнении практического задания
2	18 неделя обучения	Подготовка и сдача зачета	18	Зачет

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения «зачтено» отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка «незачтено» выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.



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»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

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

№ 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, знает	ПР-7	1-12
		ПК-14, умеет	ПР-6	1-12
		ПК-20 владеет	ПР-6	1-12
2	Раздел II. Средства защиты информации от технической разведки	ПК-12, знает	ПР-7	13-21
		ПК-14, умеет	ПР-6	13-21
		ПК-20 владеет	ПР-6	13-21

Оценочные средства для промежуточной аттестации

Список вопросов на зачёт

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.

Критерии выставления оценки на зачет

Оценка	Требования к сформированным компетенциям
«зачтено»	Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«не зачтено»	Оценка «не зачтено» выставляется студенту, который не знает значительной

	части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.
--	--

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	ПР-6	Лабораторная работа	Средство для закрепления и практического освоения материала по определенному разделу	Комплект лабораторных заданий
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины