МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Защита информации в системах беспроводной связи» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (утв. приказом Минобрнауки России от 19.09.2017г. №930) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Етчо С.А.

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FEF817
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Цели дисциплины:

Формирование у студентов комплекса знаний, умений и навыков в области обеспечения информационной безопасности в системах беспроводной связи, изучение принципов построения защищенных распределенных инфокоммуникационных систем и освоение методов противодействия угрозам в беспроводных каналах передачи данных.

Задачи дисциплины:

1. Изучение современных технологий и протоколов беспроводной передачи данных, их архитектуры и классификации.
2. Выявление и анализ основных угроз информации в системах беспроводной связи (перехват, отказ в обслуживании, подмена базовой станции и др.).
3. Изучение программно-аппаратных средств обеспечения безопасности в беспроводных сетях с учетом необходимости импортозамещения.
4. Формирование навыков проектирования, настройки и аудита защищенных беспроводных сетей с использованием отечественного и открытого программного обеспечения.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-3 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКВ-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации	РД1	Знание	Принципы передачи информации в радиоэфире, методы модуляции и доступа к среде
		ПКВ-3.3к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД2	Умение	Конфигурировать защищенные протоколы и межсетевые экраны для беспроводных сетей.
		ПКВ-3.4к : Оценивает эффективность и	РД3	Умение	Использовать отечественные аналоги для

		надежность защиты вычислительных сетей, операционных систем и баз данных			тестирования безопасности (аудит WPS, WPA/WPA2)
			РД4	Навык	проведения полевых испытаний и аудита защищенности беспроводных сетей

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Настойчивость и упорство в достижении цели
Формирование духовно-нравственных ценностей		
Формирование ответственного отношения к труду	Взаимопомощь и взаимоуважение	Внимательность к деталям
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Служение Отечеству и ответственность за его судьбу	Креативное мышление
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Взаимопомощь и взаимоуважение	Активная жизненная позиция

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений. Дисциплина базируется на знаниях, полученных при изучении «Основы информационной безопасности», «Защита информации от утечки по техническим каналам». Знания, полученные в ходе изучения дисциплины, необходимы для выполнения выпускной квалификационной работы.

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
11.03.02 Инфокоммуникационные технологии и системы связи	ОФО	Б1.В	7	5	33	16	16	0	1	0	147	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Особенности беспроводных технологий	РД1, РД2, РД3	4	4	0	37	практическое задание, тест
2	Виды беспроводных сетей. Основные угрозы.	РД1, РД2, РД3, РД4	4	4	0	37	практическое задание, тест
3	Построение защищенных систем	РД1, РД2, РД3	4	4	0	37	практическое задание, тест
4	Методика испытаний систем.	РД1, РД2, РД3, РД4	4	4	0	37	практическое задание, тест
Итого по таблице			**16**	**16**	**0**	**148**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Особенности беспроводных технологий.

Содержание темы: Основы и особенности беспроводных технологий. История развития. Отличия от проводных технологий. Классификация (WLAN, WPAN, WWAN). Принципы передачи информации в радиоэфире. Пакетная передача. Методы модуляции (OFDM, DSSS). Методы доступа к среде (CSMA/CA, FDMA, TDMA) .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Виды беспроводных сетей. Основные угрозы.

Содержание темы: Стандарты IEEE 802.11. Архитектура сети (BSS, ESS). Угрозы: подслушивание, отказ в обслуживании (DoS), глушение, атаки на криптозащиту (WEP, WPA/WPA2), уязвимости WPS.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Построение защищенных систем.

Содержание темы: Принципы проектирования. Аутентификация (802.1X/EAP). Криптографические алгоритмы (AES, ГОСТ 28147-89). Инфраструктура открытых ключей (PKI). Применение отечественных СКЗИ.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Методика испытаний систем.

Содержание темы: Факторы производительности. Рекомендуемый комплекс полевых испытаний. Методика оценки уровня защищенности. Использование анализаторов спектра и Wi-Fi анализаторов.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Данилов, С. Н. Современные методы криптографии и кодирования : учебное пособие / С. Н. Данилов. – Москва ; Вологда : Инфра-Инженерия, 2025. - 108 с. – ISBN 978-5-9729-2620-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2225349 (дата обращения: 31.05.2026)

2. Тихвинский, В. О. Информационная безопасность сетей мобильной связи 5G : учебное пособие / В. О. Тихвинский, Е. Е. Девяткин. – Москва : Издательско-торговая корпорация «Дашков и К°», 2026. - 264 с. – ISBN 978-5-394-06413-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2242873 (дата обращения: 31.05.2026)

3. Файзуллин, Р. Р. Теоретические основы передачи информации в системах беспроводной связи с кодовым разделением каналов : учебное пособие / Р. Р. Файзуллин, И. М. Лернер, И. В. Рябов. – Москва ; Вологда : Инфра-Инженерия, 2025. - 124 с. – ISBN 978-5-9729-2419-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2226299 (дата обращения: 31.05.2026)

7.2 Дополнительная литература

1. Казарин О. В., Забабурин А. С. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебник и практикум для вузов [Электронный ресурс] : Москва : Издательство Юрайт , 2022 - 312 -

Режим доступа: https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-491249

2. Поздняк, И. С. Методические рекомендации по выполнению лабораторных работ по дисциплине «Защита информации в системах беспроводной связи» : учебно-методическое пособие / И. С. Поздняк, И. С. Макаров, С. А. Жулев. — Самара : ПГУТИ, 2023. — 28 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/411839 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

3. СПС Консультант Плюс

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Электронно-библиотечная система ЮРАЙТ - Режим доступа: https://urait.ru/
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Office 2013 Suites and Apps KMS

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-3 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКВ-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации
		ПКВ-3.3к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
		ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-3 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-3.2к : Знает современную эталонную модель взаимодействия открытых систем, принципы построения и функционирования систем и сетей передачи информации	РД 1	Знание	Принципы передачи информации в радиоэфире, методы модуляции и доступа к среде	тест
ПКВ-3.3к : Использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД 2	Умение	Конфигурировать защищенные протоколы и межсетевые экраны для беспроводных сетей.	выполнение практических заданий
ПКВ-3.4к : Оценивает эффективность и надежность защиты вычислительных сетей, операционных систем и баз данных	РД 3	Умение	Использовать отечественные аналоги для тестирования безопасности (аудит WPS, WPA/WPA2)	выполнение практических заданий

	РД 4	Навык	проведения полевых испытаний и аудита защищенности беспроводных сетей	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : Принципы передачи информации в радиоэфире, методы модуляции и доступа к среде	1.1. Особенности беспроводных технологий	Тест	Экзамен в устной форме
		1.2. Виды беспроводных сетей. Основные угрозы.	Тест	Экзамен в устной форме
		1.3. Построение защищенных систем	Тест	Экзамен в устной форме
		1.4. Методика испытаний систем.	Тест	Экзамен в устной форме
РД2	Умение : Конфигурировать защищенные протоколы и межсетевые экраны для беспроводных сетей.	1.1. Особенности беспроводных технологий	Практическая работа	Экзамен в устной форме
		1.2. Виды беспроводных сетей. Основные угрозы.	Практическая работа	Экзамен в устной форме
		1.3. Построение защищенных систем	Практическая работа	Экзамен в устной форме
		1.4. Методика испытаний систем.	Практическая работа	Экзамен в устной форме
РД3	Умение : Использовать отечественные аналоги для тестирования безопасности (аудит WPS, WPA/WPA2)	1.1. Особенности беспроводных технологий	Практическое задание	Экзамен в устной форме
		1.2. Виды беспроводных сетей. Основные угрозы.	Практическое задание	Экзамен в устной форме
		1.3. Построение защищенных систем	Практическое задание	Экзамен в устной форме
		1.4. Методика испытаний систем.	Практическое задание	Экзамен в устной форме
РД4	Навык : проведения полевых испытаний и аудита защищенности беспроводных сетей	1.2. Виды беспроводных сетей. Основные угрозы.	Практическая работа	Экзамен в устной форме
		1.4. Методика испытаний систем.	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		60		60
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры тестовых заданий

Вопрос: Взаимное увеличение или уменьшение результирующей амплитуды двух или нескольких когерентных волн при их наложении друг на друга называется …

- A. Резонанс
- B. Интерференция
- C. Эффект «бегущей волны»
- D. Эффект «стоячей волны»

Вопрос: Какой метод доступа к среде передачи данных используется в сетях стандарта IEEE 802.11?

- A. CSMA/CD
- B. Token Passing

- C. CSMA/CA
- D. Polling

Вопрос: Блок данных, формируемый протоколом IP в сетях передачи данных, принято называть:

- A. Бит
- B. Кадр (Frame)
- C. Пакет (Packet)
- D. Сегмент (Segment)

Вопрос: Какая международная организация в настоящее время отвечает за выделение уникальных глобальных IP-адресов в сети Интернет?

- A. IEEE
- B. ISO
- C. ICANN
- D. ETSI

Вопрос: Какой из перечисленных протоколов аутентификации используется в защищенных беспроводных сетях корпоративного уровня в рамках стандарта IEEE 802.1X?

- A. PAP
- B. CHAP
- C. EAP (Extensible Authentication Protocol)
- D. PPP

Вопрос: Согласно стандарту IEEE 802.11, какую функцию выполняет роль «Аутентификатор (Authenticator)»?

- A. Запрашивает доступ к беспроводной сети и отвечает на запросы точки доступа
- B. Управляет физическим доступом к сети на основе статуса аутентификации клиента
- C. Выполняет фактическую проверку подлинности клиента и сообщает точке доступа о предоставлении или отказе в доступе
- D. Инициирует процесс аутентификации

Вопрос: Какое из перечисленных программных средств относится к классу открытого (Open Source) ПО и широко используется для тестирования защищенности беспроводных сетей, включая словарные атаки на WPA/WPA2?

- A. Microsoft Windows Defender
- B. Kaspersky Endpoint Security
- C. Kali Linux (с пакетом Aircrack-ng)
- D. Adobe Photoshop

Вопрос: В условиях санкционных ограничений и политики импортозамещения, какой из перечисленных программно-аппаратных комплексов является отечественным средством криптографической защиты информации (СКЗИ) и может применяться для шифрования каналов связи в защищенной инфокоммуникационной инфраструктуре?

- A. Cisco ASA

- B. Check Point NGFW
- C. ФПСУ-IP (программно-аппаратный комплекс шифрования)
- D. MikroTik RouterOS

Вопрос: Риск информационной безопасности в контексте оценки эффективности защиты вычислительных сетей определяется как:

- A. Количество уязвимостей в системе защиты
- B. Стоимость средств защиты информации
- C. Сочетание вероятности реализации угрозы и величины возможного ущерба от ее реализации
- D. Время, необходимое злоумышленнику для взлома системы

Вопрос: Метод обнаружения вторжений, основанный на сравнении сетевого трафика с ранее известными шаблонами (сигнатурами) атак, характеризуется следующим недостатком:

- A. Сложность настройки для конечного пользователя
- B. Невозможность обнаружения ранее неизвестных (zero-day) атак
- C. Высокая нагрузка на процессор
- D. Высокая стоимость лицензий

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Практическая работа № 1

Исследование потоков данных и механизмов взаимодействия в Wi-Fi сетях

Цель работы: Изучить структуру кадров беспроводной сети стандарта IEEE 802.11, освоить базовые приемы анализа сетевого трафика и идентификации устройств в эфире.

Задачи:

Установить и настроить программу-анализатор трафика (Wireshark) в среде Linux (Kali / Astra Linux).

Перевести Wi-Fi адаптер в режим мониторинга (monitor mode).

Выполнить захват трафика в беспроводной сети.

Провести анализ захваченных кадров:

Определить SSID и BSSID (MAC-адрес точки доступа).

Идентифицировать типы кадров (Beacon, Probe Request/Response, Authentication, Association).

Найти MAC-адреса клиентских устройств.

Определить используемый протокол безопасности (Open, WEP, WPA/WPA2) по полям фреймов.

Составить отчет о структуре сети и используемых протоколах.

Практическая работа № 2

Словарные атаки на сети стандарта WPA/WPA2 с использованием открытого и отечественного ПО

Цель работы: Изучить уязвимости протокола WPA/WPA2-PSK к словарным атакам, освоить методику проведения атак и выработать рекомендации по защите.

Задачи:

Настроить тестовую точку доступа с WPA2-PSK (известный пароль).

Использовать инструменты пакета aircrack-ng для захвата 4-стороннего рукопожатия (EAPOL handshake).

Провести словарную атаку с использованием стандартного словаря (rockyou.txt) и собственного небольшого словаря.

Проанализировать скорость перебора и факторы, влияющие на успех атаки (длина пароля, сложность, мощность GPU).

Рассмотреть возможность использования отечественных средств криптозащиты для повышения стойкости парольной защиты (использование российских алгоритмов хэширования по ГОСТ Р 34.11-2012).

Сформулировать политику парольной безопасности для беспроводных сетей организации.

Практическая работа № 3

Атака типа «Отказ в обслуживании» (De-Authentication Flood). Методы обнаружения и защиты

Цель работы: Изучить механизм деаутентификации клиентских устройств в Wi-Fi сетях, освоить методику проведения DoS-атаки, научиться обнаруживать такие атаки с помощью систем мониторинга и настраивать защитные механизмы.

Задачи:

Изучить формат кадра De-Authentication в стандарте IEEE 802.11.

Использовать утилиту aireplay-ng (или mdk4) для отправки потока De-Auth кадров от имени легитимной точки доступа.

Наблюдать эффект атаки – отключение клиентских устройств от сети.

Настроить мониторинг трафика для обнаружения аномального количества De-Auth кадров.

Изучить механизмы защиты:

Использование протокола 802.11w (Management Frame Protection).

Настройка IDS/IPS на точке доступа (например, отечественные системы обнаружения вторжений).

Проверить эффективность защитных механизмов путем повторного проведения атаки.

Практическая работа № 4

Комплексный аудит безопасности беспроводной локальной сети с оформлением акта тестирования

Цель работы: Систематизировать знания по аудиту защищенности беспроводных сетей, выполнить полный цикл тестирования безопасности, оформить профессиональное заключение (акт) по результатам аудита.

Задачи:

Провести пассивный анализ эфира (сбор информации о точках доступа и клиентах, определение используемых протоколов, шифрования).

Выполнить активное тестирование безопасности:

Проверить уязвимости протокола WPS (используя reaver / bully).

Выполнить атаку на WPA/WPA2-PSK (захват рукопожатия + словарная атака).

Проверить наличие открытых (незащищенных) сетей.

Проверить возможность проведения атаки De-Authentication.

Оценить стойкость сети к атакам с использованием рентгеновского анализатора спектра (при наличии оборудования).

Проанализировать используемые средства криптографической защиты с точки зрения соответствия требованиям ФСТЭК / ФСБ России.

Оформить акт тестирования безопасности беспроводной сети с выявленными уязвимостями и рекомендациями по их устранению.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

1. Основные отличия беспроводных технологий передачи данных от проводных. Классификация беспроводных технологий по дальности действия, топологии и области применения.
2. Принципы передачи информации в радиоэфире: синхронизация, пакетная передача, методы модуляции и методы доступа к среде.
3. Архитектура беспроводных локальных сетей стандарта IEEE 802.11. Режимы работы (Ad-hoc, Infrastructure). Базовый набор услуг (BSS) и расширенный набор услуг (ESS).
4. Основные угрозы информационной безопасности в системах беспроводной связи: подслушивание (Eavesdropping), отказ в обслуживании (DoS), глушение (Jamming), атаки на криптозащиту.
5. Стандарты и протоколы аутентификации в беспроводных сетях: WPA, WPA2, WPA3. Протокол IEEE 802.1X/EAP. Сравнительный анализ безопасности.
6. Инфраструктура открытых ключей (PKI) и её роль в обеспечении безопасности беспроводных корпоративных сетей. Цифровой сертификат, удостоверяющий центр (УЦ).
7. Отечественные средства криптографической защиты информации (СКЗИ) для беспроводных сетей. Стандарты ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.
8. Методика тестирования защищенности беспроводных сетей. Пассивный и активный аудит. Инструментарий: анализаторы спектра, анализаторы Wi-Fi трафика, системы обнаружения вторжений (IDS/IPS).
9. Атаки типа «отказ в обслуживании» (DoS) на беспроводные локальные сети. Механизмы реализации (De-Authentication Flood, Beacon Flood, Authentication Flood) и методы защиты (802.11w, MFP, IDS/IPS).
10. Обеспечение безопасности в сетях интернета вещей (IoT) с беспроводными интерфейсами (ZigBee, Bluetooth, LoRaWAN, NB-IoT). Специфика угроз и методов защиты.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» 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.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.