

**ГОУ ВПО Российско-Армянский (Славянский)
университет**

Утверждено

Директор Института
Агаронян А.К.



«30» апреля 2025 г., протокол № 05
Утвержден Ученым Советом ИФИ

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

**Наименование дисциплины: Б1.В.ДВ.02.02 Защита информации
телекоммуникационных систем**

Автор (ы) д.т.н., профессор Маркосян М.В.
Ф.И.О, ученое звание (при наличии), ученая степень (при наличии)

**Направление подготовки: _11.03.02 Инфокоммуникационные
технологии и системы связи**

Согласовано:

Вр. и.о. заведующего Кафедрой Телекоммуникаций
Сиволенко Э. Р.



(подпись)

1. АННОТАЦИЯ

- 1.1.** В курсе дисциплины “Защита информации телекоммуникационных систем” излагаются основные понятия информационной безопасности, необходимые для профессиональной деятельности в области информационных технологий и систем связи. Рассматриваются основные угрозы и методы защиты от них. Приводятся средства, принципы и механизмы обеспечения информационной безопасности. Даны определения и примеры криптографического закрытия информации. Подробно рассмотрены симметричные и асимметричные криптосистемы, методы создания цифровой подписи, специальные технические средства для защиты помещений и аппаратуры.
- 1.2.** Трудоемкость в академических кредитах 3 и часах - 108, формы итогового контроля зачет;
- 1.3.** Взаимосвязь дисциплины с другими дисциплинами учебного плана специальности (направления) Данная дисциплина теснейшим образом связана со следующими дисциплинами: теория информации, теория кодирования, общая теория связи, построение телекоммуникационных сетей и систем.
- 1.4.** Результаты освоения программы дисциплины:

Код компетенции (в соответствии рабочим с учебным планом)	Наименование компетенции (в соответствии рабочим с учебным планом)	Код индикатора достижения компетенций (в соответствии рабочим с учебным планом)	Наименование индикатора достижений компетенций (в соответствии рабочим с учебным планом)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 УК-1.2	Знает методики поиска, сбора и обработки информации, метод системного анализа Умеет применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников, применять системный подход для

		УК-1.3	решения поставленных задач. Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач.
ПК-3	Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований	ПК-3.1 ПК-3.2 ПК-3.3	Знает основы сетевых технологий, нормативно-техническую документацию, требования технических регламентов, международные и национальные стандарты в области качественных показателей работы инфокоммуникационного оборудования Умеет работать с программным обеспечением, используемым при обработке информации инфокоммуникационных систем и их составляющих Владеет навыками анализа оперативной информации о запланированных и аварийных работах, связанных с прерыванием предоставления услуг, контроля качества предоставляемых услуг

2. УЧЕБНАЯ ПРОГРАММА

2.1. Цель дисциплины – ознакомление студентов с основными понятиями и определениями информационной безопасности, необходимыми для профессиональной деятельности в области информационных технологий и

телекоммуникаций. Изучение различных методов криптографического закрытия информации, грамотного выбора паролей и способов постановки цифровой подписи.

Задача - ознакомление студентов с проблемой обеспечения безопасности информационных систем, изучение различных угроз и методов защиты от них..

2.2. Трудоемкость дисциплины и виды учебной работы (в академических часах и зачетных единицах) (удалить строки, которые не будут применены в рамках дисциплины)

Виды учебной работы	Всего, в акад. часах	Распределение по семестрам					
		III сем	_IV_ сем	_V_ сем	_VI_ сем	VII сем	VIII сем
1	2	3	4	5	6	7	8
1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:	108					108	
1.1. Аудиторные занятия, в т. ч.:	48					48	
1.1.1. Лекции	16					16	
1.1.2. Практические занятия, в т. ч.	32					32	
1.1.2.1. Обсуждение прикладных проектов	16					16	
1.1.2.2. Кейсы							
1.1.2.3. Деловые игры, тренинги							
1.1.2.4. Контрольные работы	16					16	
1.1.2.5. Другое (указать)							
1.1.3. Семинары							
1.1.4. Лабораторные работы							
1.1.5. Другие виды (указать)							
1.2. Самостоятельная работа, в т. ч.:	60					60	
1.2.1. Подготовка к экзаменам							
1.2.2. Другие виды самостоятельной работы, в т.ч. (указать)							
1.2.2.1. Письменные домашние задания							
1.2.2.2. Курсовые работы							
1.2.2.3. Эссе и рефераты							
1.2.2.4. Другое (указать)							
1.3. Консультации							
1.4. Другие методы и формы занятий							
Итоговый контроль (Экзамен, Зачет, диф. зачет - указать)	Зачет					Зачет	

2.3. Содержание дисциплины

2.3.1. Тематический план и трудоемкость аудиторных занятий (модули, разделы дисциплины и виды занятий) по рабочему учебному плану

Разделы и темы дисциплины	Всего (ак. часов)	Лекционные занятия (ак. часов)	Семинарские занятия (ак. часов)	Практические занятия (ак. часов)	Лабораторные работы (ак. часов)
1	2	3	4	5	6
МОДУЛЬ 1. ВИДЫ УГРОЗ. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	16	6			10
Введение. Постановка проблемы информационной безопасности	1	1	-	-	-
Раздел 1. Основные виды угроз					
<i>Тема 1.1. Естественные и искусственные угрозы.</i>	3	1			2
<i>Тема 1.2. Случайные и преднамеренные угрозы. Виды преднамеренных угроз</i>	3	1			2
Раздел 2. Система информационной безопасности	-	-	-	-	-
<i>Тема 2.1. Средства обеспечения информационной безопасности.</i>	3	1	-	-	2
<i>Тема 2.2 Принципы построения системы информационной безопасности.</i>	3	1	-	-	2
<i>Тема 2.3. Механизмы обеспечения информационной безопасности.</i>	3	1			2
МОДУЛЬ 2 КРИПТОГРАФИЯ И ЦИФРОВАЯ ПОДПИСЬ	10	4			6
Раздел 3. Криптографическое закрытие информации.					
<i>Тема 3.1. История развития криптографии. Симметричные и асимметричные системы.</i>	1	1			-
<i>Тема 3.2. Работы Шеннона по теории организации секретной связи.</i>	3	1			2
Раздел 4.Электронная цифровая подпись .					
<i>Тема 4.1. Различия между обычной и цифровой подписями.</i>	3	1			2
<i>Тема 4.2.Криптографические хеш-функции.</i>	3	1			2
МОДУЛЬ 3. ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМ И ЭТАПЫ РАЗРАБОТКИ ЗАЩИТЫ	8	2	-	-	6

Раздел 5. Оценка безопасности информационных систем.	-	-	-	-	-
<i>Тема 5.1. Подходы к оценке безопасности в США и России</i>	1	1	-	-	-
<i>Тема 5.2. Показатели защищенности.</i>	3	1	-	-	2
Раздел 6. Этапы разработки системы защиты.			-		
<i>Тема 6.1. Выявление потенциальных угроз и определение способов защиты.</i>	5	1	-	-	4
МОДУЛЬ 4.ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	14	4			10
Раздел 7. Специальные средства защиты.					
<i>Тема 7.1. Защита помещений от подслушивания.</i>	3	1			2
<i>Тема 7.2.Защита аппаратуры и коммуникаций</i>	4	1			3
МОДУЛЬ 5 СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					
Раздел 8 Внешние и внутренние угрозы.					
<i>Тема 8.1.Защита беспроводных сетей.</i>	4	1			3
<i>Тема 8.2. Защита от внешних и внутренних угроз.</i>	3	1			2
ИТОГО:	48	16			32

2.3.2. Краткое содержание разделов дисциплины в виде тематического плана

МОДУЛЬ 1. ВИДЫ УГРОЗ. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Постановка проблемы информационной безопасности. Объективные причины роста актуальности этой проблемы. Содержание дисциплины. (3: Гл 1)

Раздел1. Основные виды угроз

Тема 1.1. Естественные и искусственные угрозы

Стихийные бедствия и аварии. Сбои и отказы технических средств и программного обеспечения. Ошибки проектирования и эксплуатации. (4:Гл6 § 6:1:2)

Тема 1.2. Случайные и преднамеренные угрозы. Виды преднамеренных угроз.

Физическое разрушение и хищения. Подслушивание и подглядывание. Вербовка персонала. Перехват данных и побочных излучений. Внедрение жучков и программных закладок. (4 Гл 6 § 6:1:2)

Раздел 2. Система информационной безопасности

Тема 2.1. Средства обеспечения информационной безопасности

Правовые, морально-этические, организационные, физические, технические.

Тема 2.2. Принципы построения системы информационной безопасности

Системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость, простота (2. Гл2)

Тема 2.3 Механизмы обеспечения информационной безопасности

Идентификация, аутентификация, авторизация, контроль доступа, регистрация и анализ событий, контроль целостности ресурсов.(1 Гл 2§ 2.1)

МОДУЛЬ 2. КРИПТОГРАФИЯ И ЦИФРОВАЯ ПОДПИСЬ

Раздел 3. Криптографическая защита информации

Тема 3.1.История развития криптографии

Древняя Греция и Рим. Шифровальный диск Альберти, черные кабинеты, гаммирование, колесные шифраторы, шифры перестановки. Криптография с открытыми ключами
(1 Глава 1)

Тема 3.2.Работы Шеннона по теории кодирования

Анализ шифра по открытому сообщению и расстояние единственности. (1 Глава 1)

Раздел 4. Электронная цифровая подпись

Тема 4.1. Различия между обычной и цифровой подписями

Обычная подпись всегда одинакова, связана с подписывающим лицом, не требует для реализации дополнительных механизмов и структур.(1, Гл14 § 14:..1)

Цифровая подпись всегда разная, определяется секретным ключом, требует создания алгоритмов вычисления и проверки

Тема 4.2. Криптографический Хэш-функции

Применение Хэш-функций для контроля целостности данных и аутентификации источника данных. Построение Хэш-функций. (1: Гл13 § 13. 2.,13 3)

МОДУЛЬ 3. ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМ И ЭТАПЫ

РАЗРАБОТКИ ЗАЩИТЫ

Раздел 5. Оценка безопасности информационных систем

Тема 5.1. Подходы к оценке безопасности в США и России

Уровни безопасности согласно “Оранжевой книге”. Стандарт TEMPEST. Политика безопасности. Документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации ..(6 Гл 6 § 6, 2.1)

Тема 5.2. Показатели защищенности

Средства, влияющие на защищенность систем и оцениваемые группой требований варьируемых по уровню и глубине в зависимости от класса защиты. ..(6 Гл 6 § 6, 2. 2)

Раздел 6. Этапы разработки системы защиты

Тема 6.1. Выявление потенциальных угроз и определение способов защиты

Разработка плана защиты и формирование политики безопасности. Построение системы информационной безопасности. Контроль и доведение до персонала реализуемых мер безопасности. ..(6 Гл 6 § 6, 2.5) (7)

МОДУЛЬ 4. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Раздел 7. Специальные средства защиты.

Тема 7.1. Защита помещений от подслушивания

Звукоизоляция стен, полов, потолков, тамбуры, специальные стекла, шторы, фильтры

Тема 7.2. Защита аппаратуры и коммуникаций

Портативные детекторы локаторы излучений. Генераторы помех.. Аппаратура для защиты телефонов .

МОДУЛЬ 5. СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Раздел 8. Внешние и внутренние угрозы

Тема 8.1. Защита проводных и беспроводных сетей

Обеспечение конфиденциальности информации и защита от искажений.

Тема 8.2. Защита от внешних и внутренних угроз

Компьютерные вирусы, сетевые черви и троянские программы. Защита от инсайдеров

Наименование лабораторных работ
1. Шифр Цезаря..
2. Шифр простой замены..
3. Шифр Плейфера. .
4. Книжные шифры. .
5. Алгоритм Диффи и Хеллмана..
6. Алгоритм RSA..
7. Хеш-функции.
8. Цифровая подпись..
9. Фишинг и методы социальной инженерии

2.4. Материально-техническое обеспечение дисциплины

- Учебные методические пособия
- Вычислительная техника
- Проектор
- Слайдоскоп

2.5. Распределение весов по модулям и формам контроля

Формы контролей	Веса форм текущих контролей в	Веса форм промежуточных контролей в	Веса оценок промежуточных контролей и	Веса итоговых оценок	Веса результирующей оценки
-----------------	-------------------------------	-------------------------------------	---------------------------------------	----------------------	----------------------------

	результатирующих оценках текущих контролей			оценках промежуточных контролей			результатирующих оценок текущих контролей в итоговых оценках промежуточных контролей			промежуточ ных контролей в результатиру ющей оценке промежуточ ных контролей	промежуточных контролей и оценки итогового контроля в результатирующей оценке итогового контроля
Вид учебной работы/контроля	M1 ¹	M2	M3	M1	M2	M3	M1	M2	M3		
Контрольная работа											
Тест											
Курсовая работа											
Лабораторные работы		1	1								
Письменные домашние задания											
Реферат											
Эссе											
Семинары											
Решение задач											
Весы результирующих оценок текущих контролей в итоговых оценках промежуточных контролей								1	1		
Весы оценок промежуточных контролей в итоговых оценках промежуточных контролей											
Вес итоговой оценки 1-го промежуточного контроля в результатирующей оценке промежуточных контролей										-	
Вес итоговой оценки 2-го промежуточного контроля в результатирующей оценке промежуточных контролей										0.5	
Вес итоговой оценки 3-го промежуточного контроля в результатирующей оценке промежуточных контролей										0.5	
Вес результирующей оценки промежуточных контролей в результатирующей оценке итогового контроля											1
Экзамен/зачет (оценка итогового контроля)											0 (Зачет) 0.6
	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$	$\Sigma = 1$

3. Теоретический блок

Рекомендуемая литература

а) Базовые учебники

1. А.П. Алферов, А.Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин Основы криптографии Учебное пособие М Гелиос 2001:
2. В.И. Таирян. Основы информационной безопасности в компьютерных сетях Учебное пособие Изд РАУ 2006.

б) Дополнительная литература:

3. В. И. Ярочкин Информационная безопасность. М. Академический проект 2005
4. Информационные технологии управления. Учебное пособие для вузов. М, ЮНИТИ 2003
5. В. Безмалый Служба защиты информации первые шаги Компьютер Пресс №3 2008.
6. С. Шляхтина .И Т безопасность сегодня и завтра Компьютер Пресс №3 2008.
7. В.В. Мартынов Организация системы информационной безопасности Вестник МАНЭБ том14 № 4 Выпуск 2009..
8. В. В. Мартынов Защита информации при помощи паролей. Изв. Арм. научно-технич. Академии № 3 2010.
9. В. В. Мартынов Безопасность беспроводных сетей. Доклады международной научно-практической конференции по вопросам безопасности информационных систем. Ереван, Тигран Мец 2011

4. Перечень вопросов итогового контроля .

1. Постановка проблемы информационной безопасности. Причины повышения остроты этой проблемы.
2. Понятие угрозы. Классификация угроз по природе их возникновения и мотивации действий
3. Преднамеренные пассивные угрозы. Примеры пассивных угроз.
4. Преднамеренные активные угрозы. Примеры активных угроз.
5. Правовые и морально-этические средства обеспечения информационной безопасности.
6. Организационные средства обеспечения информационной безопасности .
7. Физические и технические средства обеспечения информационной безопасности.
8. Принципы системности и комплексности построения системы информационной безопасности.

9. Принципы непрерывности и разумной достаточности построения системы информационной безопасности.
10. Принципы гибкости, открытости алгоритмов и простоты применения построения системы информационной безопасности. .
11. Идентификация - процесс распознавания субъектов и объектов.
12. Аутентификация - проверка подлинности идентификации.
13. Авторизация - предоставление субъектам прав на доступ.
14. Четыре основных способа разделения доступа к совместно используемым объектам.
15. Механизм регистрации и контроля целостности.
16. Криптография Обеспечение конфиденциальности целостности невозможности отказа от авторства
17. Квадрат Полибия и табличка Энея .
18. Таблица Тритемия и решетка Кардана
- !9. Шифры Решелье и Гронсфельда
20. Колесные шифраторы .
21. Шифры перестановки
22. Симметричные и асимметричные системы
23. Цифровая подпись Различия между обычной и цифровой подписями .
24. Криптографические Хэш-функции
- 25 Подходы к оценке безопасности в США России
26. Этапы разработки системы информационной безопасности
27. Современные вредоносные программы
28. Защита от инсайдеров