

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра цифровых технологий и машинного обучения

УТВЕРЖДАЮ

Декан физического факультета



И.С. Огнев

«23» мая 2023 г.

Рабочая программа дисциплины
«Защищенные системы связи»

Направление подготовки
11.04.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль)
«Сети, системы и устройства телекоммуникаций»

Форма обучения
очная

Программа рассмотрена
на заседании кафедры
от «17» апреля 2023 года, протокол № 8

Программа одобрена НМК
физического факультета
протокол № 5 от «25» апреля 2023 года.

Ярославль

1. Цели освоения дисциплины

Цель курса – научить студентов основным принципам и методам, применяемым при защите систем связи.

Задачи курса:

- ознакомить студентов с основными проблемами защиты информации в телекоммуникационных системах;
- показать основные методы и средства, используемые при защите систем передачи и обработки информации;
- обучить студентов стандартным приемам защиты информации в компьютерных системах и локальных сетях.

Дисциплина «Защищенные системы связи» обеспечивает формирование представлений о принципах функционирования и подходах к построению защищенных систем связи, их особенностях, современных тенденциях, проблемах и перспективах, а также создает необходимую базу для успешного решения профессиональных задач.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору.

Она основывается на знаниях, умениях и навыках, полученных студентами при изучении дисциплин: «Математическое моделирование устройств и систем», «Радиотехнические и телекоммуникационные системы», «Теория построения информационных систем и сетей», «Системы и сети связи с подвижными объектами».

Она тесно связана с дисциплиной «Обеспечение информационной безопасности в информационных сетях», а также с рядом дисциплин по выбору.

Знания, умения и навыки, полученные при изучении данной дисциплины, могут использоваться студентами при выполнении выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции		
ПК-2. Способен к организации и самостоятельному выполнению фундаментальных и (или) прикладных исследований теоретического и (или) экспериментального характера	ИД_ПК-2.2 Самостоятельно выполняет исследования теоретического и (или) экспериментального характера в соответствии с планом	Знать: технологию построения защищенных систем связи, методы оценок защищенности телекоммуникационных систем, основные методы атак на телекоммуникационное оборудование и сервисы, основные методы защит от атак на телекоммуникационное оборудование и сервисы Уметь: оценивать защищенность систем связи, выявлять и устранять потенциально опасные с позиций безопасности места системы Владеть навыками: методами сбора и анализа информации, необходимой для оценки защищенности телекоммуникационных систем, навыками работы с нормативными документами по оценке защищенности компьютерных систем

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Введение	3		2				6,7	Устный опрос
2	Технологии защиты информации	3		6		1		16	Устный опрос
3	Стандарты по защите информации.	3		5		1		12	Устный опрос
4	Общие критерии оценки защищенности телекоммуникационных систем	3		5		1		16	Устный опрос
		3					0,3		Зачет
	Всего с зачетом	3		18		3	0,3	50,7	

Содержание разделов дисциплины

Тема № 1

Введение

Основные понятия

Роль специалистов по организации защиты информации в государственных и коммерческих структурах.

Информационные технологии и информационные системы.

Примеры информационных технологий: SAP/R3, операционный день банка, рабочее место брокера.

Тема № 2

Технологии защиты информации

Основные технологии защиты информации.

Ценности, опасности, потери, риски, угрозы в компьютерных системах.

Основные угрозы информации в компьютерных системах.

Специфика возникновения угроз в открытых сетях.

Особенности защиты информации на узлах компьютерной сети.

Системные вопросы защиты программ и данных.

Анализ рисков.

Модель противника, возможности противника.

Тема № 3
Стандарты по защите информации

Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

Структуры в РФ, обеспечивающие лицензирование и сертификацию.

Тема № 4
Общие критерии оценки защищенности телекоммуникационных систем

Функциональные требования. Вопросы гарантий и эффективности.

Требования к подсистемам аудита.

Подсистемы подтверждения подлинности отправки и получения сообщения.

Подсистемы разграничения доступа.

Подсистемы аутентификации.

Подсистемы защиты функций защиты.

Подсистемы защиты ресурсов системы.

Подсистемы защиты связи.

Каналы утечки информации и их анализ.

Методология анализа гарантий.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения соответствующей дисциплине используются следующие образовательные технологии:

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекциях и в результате самостоятельной подготовки знаний.

Консультация – занятие перед проведением зачета, на котором проводится консультирование по изученному материалу, формам заданий итогового контроля, ответы на вопросы студентов по дисциплине.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniya.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Фефилов, А.Д. Методы и средства защиты информации в сетях [Электронный ресурс] / А.Д. Фефилов. - Москва: Лаборатория книги, 2011. - 105 с. URL: <http://biblioclub.ru/index.php?page=book&id=140796>

б) дополнительная литература

1. Долозов, Н.Л. Программные средства защиты информации : конспект лекций [Электронный ресурс] / Н.Л. Долозов, Т.А. Гульяева. - Новосибирск : НГТУ, 2015. - 63 с. URL: <http://biblioclub.ru/index.php?page=book&id=438307>
2. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 с. URL: <http://www.iprbookshop.ru/52161.html>
3. Титов А.А. Инженерно-техническая защита информации. [Электронный ресурс]/ А.А. Титов - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. URL: <http://biblioclub.ru/index.php?page=book&id=208567>
4. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - М.: Академия, 2006. - 331 с.
5. Хаулет, Т. Защитные средства с открытыми исходными текстами: Практическое руководство по защитным приложениям: учебное пособие [Электронный ресурс] / Т. Хаулет; под ред. В. Галатенко ; пер. с англ. В. Галатенко, О. Труфанова. - Москва : Интернет-Университет Информационных Технологий, 2007. - 608 с. - URL: <http://biblioclub.ru/index.php?page=book&id=233306>

в) ресурсы сети «Интернет»:

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uni-yar.ac.ru/opac/bk_cat_find.php).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной

техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в аудитории для практических занятий (семинаров) больше либо равно списочному составу группы обучающихся.

Автор:

Профессор кафедры инфокоммуникаций
и радиофизики, д.т.н.

_____ А.Л. Приоров

**Приложение №1 к рабочей программе дисциплины
«Защищенные системы связи»**

**Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания или иные материалы,
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,
характеризующих этапы формирования компетенций**

**1.1 Контрольные задания и иные материалы,
используемые в процессе текущей аттестации**

Устный опрос

1. Информационные технологии и информационные системы.
2. Особенности организации защиты информации в государственных и коммерческих структурах.
3. Примеры информационных технологий.
4. Проектирование и разработка информационных технологий.
5. Государственные стандарты на разработку и создание информационных систем.
6. CASE-технологии создания информационных систем.
7. Ценности, опасности, потери, риски, угрозы в компьютерных системах.
8. Основные угрозы информации в компьютерных системах.
9. Специфика возникновения угроз в открытых сетях.
10. Особенности защиты информации на узлах компьютерной сети.
11. Системные вопросы защиты программ и данных.
12. Анализ рисков.
13. Модель противника, возможности противника.
14. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
15. Анализ критических технологий.
16. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
17. Система лицензирования и сертификации средств защиты.
18. Аттестация защищенных систем.
19. Структуры в РФ, обеспечивающие лицензирование и сертификацию.
20. Нормативная база и ответственность за защиту информации в компьютерных системах.
21. Руководящий документ Гостехкомиссии по оценке защищенности АС.
22. Стандарты по защите информации.
23. Построение гарантированно защищенных баз данных и их оценка по стандарту "Оранжевая книга". Функциональные требования. Вопросы гарантий и эффективности.
24. Общие критерии оценки защищенности телекоммуникационных систем.
25. Подход к безопасности телекоммуникационных систем и базовые концепции.

26. Профиль защиты.
27. Функции поддержки политики безопасности.
28. Гарантии безопасности.
29. Требования по безопасности информационных технологий.
30. Оценки защищенности.
31. Компоненты подсистем поддержки политики безопасности.
32. Классы оценки безопасности.
33. Требования к подсистемам аудита.
34. Подсистемы подтверждения подлинности отправки и получения сообщения.
35. Подсистемы разграничения доступа.
36. Подсистемы аутентификации.
37. Подсистемы защиты функций защиты.
38. Подсистемы защиты ресурсов системы.
39. Подсистемы защиты связи.
40. Каналы утечки информации и их анализ.
41. Анализ гарантий отсутствия утечки информации.

Критерии оценивания ответов на вопросы устного опроса

Критерий	Пороговый уровень	Продвинутый уровень	Высокий уровень
Соответствие ответа вопросу	Хотя бы частичное (<i>не относящееся к вопросу не подлежит проверке</i>)	Полное	Полное
Полнота ответа	Вопрос раскрыт на 50 и более %	Ответ почти полный, без ошибок, не хватает отдельных элементов и тонкостей	Ответ полный и без ошибок

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету

1. Роль специалистов по организации защиты информации в государственных и коммерческих структурах.
2. Информационные технологии и информационные системы.
3. Примеры информационных технологий: SAP/R3, операционный день банка, рабочее место брокера.
4. Проектирование и разработка информационных технологий. Государственные стандарты на разработку и создание информационных систем.
5. CASE-технологии создания информационных систем.
6. Ценности, опасности, потери, риски, угрозы в компьютерных системах.
7. Основные угрозы информации в компьютерных системах.
8. Специфика возникновения угроз в открытых сетях.
9. Особенности защиты информации на узлах компьютерной сети.
10. Системные вопросы защиты программ и данных.
11. Анализ рисков.
12. Модель противника, возможности противника;
13. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.

14. Анализ критических технологий.
15. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
16. Система лицензирования и сертификации средств защиты. Аттестация защищенных систем.
17. Структуры в РФ, обеспечивающие лицензирование и сертификацию.
18. Нормативная база и ответственность за защиту информации в компьютерных системах.
19. Руководящий документ Гостехкомиссии по оценке защищенности АС.
20. Стандарты по защите информации.
21. Построение гарантированно защищенных баз данных и их оценка по стандарту "Оранжевая книга". Функциональные требования. Вопросы гарантий и эффективности.
22. Общие критерии оценки защищенности телекоммуникационных систем.
23. Подход к безопасности телекоммуникационных систем и базовые концепции.
24. Профиль защиты.
25. Функции поддержки политики безопасности.
26. Гарантии безопасности.
27. Требования по безопасности информационных технологий.
28. Оценки защищенности.
29. Компоненты подсистем поддержки политики безопасности.
30. Классы оценки безопасности.
31. Требования к подсистемам аудита.
32. Подсистемы подтверждения подлинности отправки и получения сообщения.
33. Подсистемы разграничения доступа.
34. Подсистемы аутентификации.
35. Подсистемы защиты функций защиты.
36. Подсистемы защиты ресурсов системы.
37. Подсистемы защиты связи.
38. Каналы утечки информации и их анализ. Методология анализа гарантий.

Критерии оценивания ответов на вопросы билета

Критерий	Пороговый уровень (на «удовлетворительно»)	Продвинутый уровень (на «хорошо»)	Высокий уровень (на «отлично»)
Соответствие ответа вопросу	Хотя бы частичное (<i>не относящееся к вопросу не подлежит проверке</i>)	Полное	Полное
Наличие примеров	Имеются отдельные примеры	Много примеров	Есть практически ко всем утверждениям
Содержание ответа	Понятийные вопросы изложены с классификациями, проблемные с постановкой проблемы и изложением различных точек зрения. Имеются ошибки или пробелы.	Ответ почти полный, без ошибок, не хватает отдельных элементов и тонкостей	Исчерпывающ ий полный ответ

2. Описание процедуры выставления оценки

Изучение дисциплины заканчивается зачетом. Для подготовки ответа на вопрос билета отводится не менее 40 минут.

Оценка «зачтено» выставляется, если ответ на вопрос билета дан не ниже, чем на пороговом уровне.

Оценка «не зачтено» выставляется, если ответ на вопрос билета дан ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины «Защищенные системы связи»

Методические указания для студентов по освоению дисциплины

Основной формой усвоения учебного материала по дисциплине «Защищенные системы связи» является самостоятельная работа студента, причем в достаточно большом объеме. По всем темам предусмотрены задания самостоятельной работы, на которых происходит закрепление изученного материала и отработка необходимых навыков.

Изучение дисциплины заканчивается зачетом. Оценка выставляется на основании уровня сформированности указанных компетенций, который оценивается как средняя оценка по совокупности параметров: оценки за самостоятельные задания и ответы на вопросы билета.

Освоить вопросы данной дисциплины самостоятельно студенту достаточно сложно. Посещение всех предусмотренных лекций и практических занятий является совершенно необходимым. Без упорных и регулярных самостоятельных занятий в течение семестра сдать зачет практически невозможно.