Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра прикладной информатики

Рабочая программа дисциплины

Б1.В.02.02 Информационная безопасность телекоммуникационных систем

Основная профессиональная образовательная программа
высшего образования по направлению подготовки

09.03.03 Прикладная информатика

Направленность (профиль)

«Прикладные информационные системы и технологии»

Уровень
Бакалавр

Форма обучения
Очная

Согласовано
Руководитель ОПОП

_____ **Колбина О.Н.**

Утверждаю
Проректор по учебной работе

_____ **Н.О. Верещагина**

Рекомендована решением
Ученного совета института Информационных систем и геотехнологий
29.06.2023 г., протокол №7

Рассмотрена и утверждена на заседании кафедры
28.06.2023 г., протокол №6
И.о. заведующего кафедрой
прикладной информатики

_____ **Истомин Е.П.**

Автор-разработчик:
к.т.н. Сидоренко А. Ю.

Санкт-Петербург 2023

1. Цель и задачи освоения дисциплины

Цель дисциплины — сформировать общепрофессиональную компетентность обучающихся в области обеспечения информационной безопасности телекоммуникационных систем, основанную на использовании принципов построения инфокоммуникационных систем, информационно-коммуникационных технологий и соблюдении основных требований информационной безопасности при решении стандартных задач профессиональной деятельности.

Задачи:

1. Сформировать знание:
   - принципов построения и функционирования телекоммуникационных и инфокоммуникационных систем;
   - основных угроз и уязвимостей информационной безопасности в телекоммуникационных системах;
     нормативных, организационных и технических требований к обеспечению информационной безопасности.
2. Сформировать умение:
   - применять информационно-коммуникационные технологии для решения стандартных профессиональных задач с учётом требований информационной безопасности;
   - анализировать структуру телекоммуникационных систем и выявлять потенциальные риски безопасности информации;
   - определять и обосновывать требования информационной безопасности для телекоммуникационных систем.
3. Сформировать владение:
   - методами и средствами обеспечения информационной безопасности в телекоммуникационных системах;
   - навыками применения организационных и технических мер защиты информации;
   - практическими навыками анализа и документирования мер по обеспечению информационной безопасности.

2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений, изучается в 4 семестре.

Изучению предшествуют следующие дисциплины:

«Иностранный язык», «Программная инженерия», «Профессиональная коммуникация системного аналитика», «Основы разработки программного обеспечения» «Архитектуры программного обеспечения», «Введение в профессиональную деятельность», «Дискретная математика для программистов», «Тайм-менеджмент», «Моделирование прикладных информационных процессов», «Информационный поиск», «Антенны и распространение радиоволн», «Введение в информационные технологии», «Системы искусственного интеллекта», «Физика квантовых компьютеров», «Методология научного исследования», «Теория вероятностей и математическая статистика», «Математические методы и модели», «ИТ и программирование».

Изучается параллельно с такими дисциплинами как:

«Объектно-ориентированное программирование», «Облачные технологии и услуги», «Разработка профессиональных приложений», «Операционные системы и компьютерные сети», «UNIX и Linux системы в инфокоммуникациях».

Дисциплина является базовой для освоения модулей и дисциплин:

«Основы проектной деятельности в профессиональной сфере», «Основы использования информационно-коммуникационных технологий для профессиональной деятельности», «Разработка визуальных систем», «Создание 1оТ-систем», «Создание пользовательских интерфейсов», «Выявление рисков создания программного продукта», «Проектирование программного обеспечения с привязкой к местности», «Сопровождение и тестирование информационных систем», «Создание и сопровождение веб-приложений», «Создание и сопровождение мультимедиа контента», «Проектирование мультимедийного программного обеспечения», «Проектирование веб-приложений», «Производственная практика (преддипломная практика)», «Выполнения и защита выпускной квалификационной работы», «Подготовка к сдаче и сдача государственного экзамена».

3. Перечень планируемых результатов обучения

Процесс изучения дисциплины направлен на формирование компетенций: ОПК-3.

Таблица 1. Компетенции

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1. Использует принципы построения инфокоммуникационных систем на основе информационной и библиографической культуры для решения стандартных задач профессиональной деятельности.	Знать: – принципов построения и функционирования телекоммуникационных и инфокоммуникационных систем. Уметь: – применять информационно-коммуникационные технологии для решения стандартных профессиональных задач с учётом требований информационной безопасности. Владеть: – методами и средствами обеспечения информационной безопасности в телекоммуникационных системах.
	ОПК-3.2. Решает стандартные задачи профессиональной деятельности в предметной области с учетом основных требований	Знать: – нормативных, организационных и технических требований к обеспечению информационной безопасности. Уметь: – определять и обосновывать требования информационной

	информационной безопасности.	безопасности для телекоммуникационных систем. Владеть: – навыками применения организационных и технических мер защиты информации.
	ОПК-3.3. Применяет основные требования информационной безопасности.	Знать: – основные угрозы и уязвимости информационной безопасности в телекоммуникационных системах. Уметь: – анализировать структуру телекоммуникационных систем и выявлять потенциальные риски безопасности информации. Владеть: – практическими навыками анализа и документирования мер по обеспечению информационной безопасности.

4. Структура и содержание дисциплины

4.1. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часов.

Таблица 2. Объем дисциплины по видам учебных занятий в академических часах

Объём дисциплины	Очная форма обучения	
	Семестр	Итого
	4 семестр	
Зачётные единицы	3	3
Контактная работа обучающихся с преподавателем (по видам аудиторных учебных занятий) – всего:	47	47
в том числе:	-	-
– лекции	18	18
– занятия семинарского типа:	28	28
практические занятия	-	-
лабораторные занятия	28	28
Самостоятельная работа (далее – СРС) – всего:	60,84	60,84
в том числе:	-	-
– курсовая работа	-	-
– контрольная работа	-	-
Контроль:		
Текущий контроль успеваемости (ТКУ)	1	1

Промежуточная аттестация	1,16	1,16
ВСЕГО ЧАСОВ:	108	108
Вид промежуточной аттестации	Зачет	Зачет

4.2. Структура тем дисциплины

Таблица 3. Структура дисциплины

№ п/п	Тема дисциплины	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля	Формируемые компетенции	Индикаторы достижения компетенций
		Лекции	Лабораторные занятия	Самостоятельная работа			
1.	Тема 1. Введение в информационную безопасность телекоммуникационных систем	4	4	12	Устная защита результатов лабораторной работы № 1	ОПК-3	ОПК-3.1 ОПК-3.2 ОПК-3.3
2.	Тема 2. Принципы построения инфокоммуникационных систем	2	4	12,84	Устная защита результатов лабораторной работы № 2	ОПК-3	ОПК-3.1 ОПК-3.2 ОПК-3.3
3.	Тема 3. Основные требования информационной безопасности	4	6	12	Устная защита результатов лабораторной работы № 3	ОПК-3	ОПК-3.1 ОПК-3.2
4.	Текущий контроль успеваемости (ТКУ)			1	Тест в Moodle	ОПК-3	ОПК-3.1 ОПК-3.2 ОПК-3.3
5.	Тема 4. Методы и средства защиты информации в телекоммуникациях	4	6	12	Устная защита результатов лабораторной работы № 4	ОПК-3	ОПК-3.1 ОПК-3.2 ОПК-3.3
6.	Тема 5. Решение стандартных задач обеспечения ИБ в телекоммуникационных системах	4	8	12	Устная защита результатов лабораторной работы № 5	ОПК-3	ОПК-3.1
-	ИТОГО	18	28	60,84	-	-	-

4.3. Содержание тем дисциплины

Таблица 4. Содержание тем дисциплины

№	Наименование темы дисциплины	Содержание	Компетенция
1	Тема 1. Введение в информационную безопасность телекоммуникационных систем	Понятие телекоммуникационных систем. Роль информационной безопасности в инфокоммуникациях. Основные угрозы и уязвимости.	ОПК-3
2	Тема 2. Принципы построения инфокоммуникационных систем	Архитектура инфокоммуникационных систем. Каналы связи, протоколы передачи данных, модели взаимодействия.	ОПК-3
3	Тема 3. Основные требования информационной безопасности	Конфиденциальность, целостность, доступность. Нормативные и организационные требования к защите информации.	ОПК-3
4	Тема 4. Методы и средства защиты информации в телекоммуникациях	Технические, программные и организационные средства защиты. Шифрование, аутентификация, контроль доступа.	ОПК-3
5	Тема 5. Решение стандартных задач обеспечения ИБ в телекоммуникационных системах	Практические сценарии обеспечения безопасности. Анализ инцидентов. Комплексный подход к защите информации.	ОПК-3

4.4. Содержание занятий семинарского типа

Таблица 5. Содержание лабораторных занятий

№ темы	Тематика лабораторных работ	Всего часов	Формируемые компетенции
1	Лабораторная работа № 1. Анализ угроз информационной безопасности телекоммуникационной системы..	4	ОПК-3
2	Лабораторная работа № 2. Изучение структуры и компонентов инфокоммуникационной системы..	4	ОПК-3
3	Лабораторная работа № 3. Определение требований информационной безопасности для телекоммуникационной системы.	6	ОПК-3
4	Лабораторная работа № 4. Выбор и обоснование средств защиты информации для телекоммуникационной системы.	6	ОПК-3
5	Лабораторная работа № 5. Разработка мер по обеспечению информационной безопасности телекоммуникационной системы.	8	ОПК-3
ВСЕГО		28	

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Электронный учебный курс «Информационная безопасность телекоммуникационных систем» в системе Moodle [Электронный ресурс]. Режим доступа: https://moodle.rshu.ru/enrol/index.php?id=1012

6. Оценочные средства для текущего контроля и промежуточной аттестации по итогам освоения дисциплины

Учет успеваемости обучающегося по дисциплине осуществляется по 100-балльной шкале.

Таблица 6. Учёт успеваемости обучающегося по дисциплине

Учет успеваемости	Количество баллов
Максимальное количество баллов по дисциплине за один семестр:	100
– максимальное количество баллов за выполнение всех видов текущего контроля	100
– максимальное количество баллов за прохождение промежуточной аттестации	30

6.1. Текущий контроль

Задания, методика выполнения и критерии оценивания текущего контроля по разделам дисциплины представлены в Фонде оценочных средств.

6.2. Промежуточная аттестация

Перечень вопросов и критерии оценивания ответов на вопросы в тесте по темам дисциплины представлены в Фонде оценочных средств по данной дисциплине.

Форма промежуточной аттестации по дисциплине: зачет.

Форма проведения зачета: тестирование.

6.3. Балльно-рейтинговая система оценивания

Таблица 7. Распределение баллов по видам учебной работы

Вид учебной работы, за которую ставятся баллы	Баллы
Текущий контроль	0-100
Промежуточная аттестация	0-30
ИТОГО	0-100

Таблица 7.1. Распределение баллов по текущему контролю

№	Вид работ	Min	Max
1. Обязательная часть			
1.1 Текущий контроль успеваемости по проверке форсированности остаточных знаний			
Текущий контроль успеваемости. Тест:		0	10
1.2 Выполнение практических работ:			
1.2.1	Лабораторная работа № 1. Анализ угроз информационной безопасности телекоммуникационной системы..	4	6

1.2.2	Лабораторная работа № 2. Изучение структуры и компонентов инфокоммуникационной системы..	4	8
1.2.3	Лабораторная работа № 3. Определение требований информационной безопасности для телекоммуникационной системы.	4	8
1.2.4	Лабораторная работа № 4. Выбор и обоснование средств защиты информации для телекоммуникационной системы.	4	10
1.2.5	Лабораторная работа № 5. Разработка мер по обеспечению информационной безопасности телекоммуникационной системы.	4	8
Итого баллов по обязательной части		20	40
2. Вариативная часть			
2.1	Реферат по дисциплине	1	4
2.2	Участие в НИРС	15	25
2.3	Участие в региональной олимпиаде по профилю	10	20
2.3.1	участие	10	10
2.3.2	призер	20	20
2.4	Публикация в индексируемом журнале (совместно с преподавателем)	10	10
2.5	Акселерационная программа/ проект Росмолодежи	20	40
2.5.1	участие	20	20
2.5.2	грант	40	40
2.6	Подготовить конспект с классификацией угроз информационной безопасности телекоммуникационных систем.	0	10
2.7	Составить структурную схему инфокоммуникационной системы с пояснением назначения её элементов.	0	10
2.8	Сформировать таблицу требований информационной безопасности (конфиденциальность, целостность, доступность) для заданной системы.	0	10
2.9	Подготовить обзор средств защиты информации в телекоммуникационных системах с указанием области применения.	0	10
2.10	Разработать текстовый отчёт с описанием комплекса мер по обеспечению информационной безопасности телекоммуникационной системы.	0	10
	Промежуточная аттестация по дисциплине	0	30
Итого баллов по вариативной части		40	60
Итого баллов по дисциплине			100

Таблица 7.2. Конвертация баллов в итоговую оценку

Оценка	Баллы
Зачтено	40-100
Не зачтено	0-39

7. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации ко всем видам аудиторных занятий, а также методические рекомендации по организации самостоятельной работы, в том числе по

подготовке к текущему контролю и промежуточной аттестации представлены в Методических рекомендации для обучающихся по освоению дисциплины.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва: Издательство Юрайт, 2023. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915

2. Нечаев, А. М. Компьютерные сети: учебник / А. М. Нечаев. — Москва: Издательство Юрайт, 2023. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/book/kompyuternye-seti-572239

3. Самуйлов, К. Е. Сети и телекоммуникации: учебник / К. Е. Самуйлов. — Москва: Издательство Юрайт, 2023. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/book/seti-i-telekommunikacii-517817

4. Основы информационной безопасности: защита информации: учебное пособие для СПО / А. А. Внуков. — Москва: Издательство Юрайт, 2022. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340

5. Организационное и правовое обеспечение информационной безопасности: учебник для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов. — Москва: Издательство Юрайт, 2022. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561717

Дополнительная литература:

1. Соколова, В. В. Вычислительная техника и информационные технологии. Разработка мобильных приложений: учебник для вузов / В. В. Соколова. — Москва: Издательство Юрайт, 2023. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561336

2. Чубукова С. Г. Правовая информатика: учебник / С. Г. Чубукова. — Москва: Издательство Юрайт, 2023. — Текст: электронно // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/index.php/book/pravovaya-informatika-580542

3. Щербак, А. В. Информационная безопасность: учебник для СПО / А. В. Щербак. — Москва: Издательство Юрайт, 2023. — Электронный ресурс // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Образовательная платформа Нетология [Электронный ресурс]. Режим доступа: https://netology.ru/
2. Образовательная платформа Яндекс Практикум [Электронный ресурс]. Режим доступа: https://practicum.yandex.ru/
3. Образовательная платформа GeekBrains [Электронный ресурс]. Режим доступа: https://gb.ru/
4. Образовательная платформа Skillbox [Электронный ресурс]. Режим доступа: https://skillbox.ru/
5. Образовательная платформа Открытое образование [Электронный ресурс]. Режим доступа: https://openedu.ru/
6. Образовательная платформа Лекториум [Электронный ресурс]. Режим доступа: https://www.lektorium.tv/
7. Виртуальная обучающая среда Moodle

8.3. Перечень программного обеспечения

1. Операционная система: Calculate linux [Электронный ресурс]. Режим доступа: https://www.calculate-linux.org/
2. Операционная система: Microsoft Windows 10 Professional [Электронный ресурс]. Режим доступа: https://www.microsoft.com/ru-ru/
3. Браузер: Яндекс браузер [Электронный ресурс]. Режим доступа: https://browser.yandex.ru/
4. Файловый архиватор: 7-zip [Электронный ресурс]. Режим доступа: https://www.7-zip.org/
5. Файловый менеджер: Far-manager [Электронный ресурс]. Режим доступа: https://farmanager.com/
6. Офисный пакет: Microsoft Office 2013 Professional [Электронный ресурс]. Режим доступа: https://www.microsoft.com/ru-ru/
7. Кроссплатформенная интегрированная среда разработки Pycharm для языка программирования Python [Электронный ресурс]. Режим доступа: https://www.jetbrains.com/pycharm/

8.4. Перечень информационных справочных систем

1. Веб-геоинформационная платформа [Электронный ресурс]. Режим доступа: https://kosmosnimki.ru/
2. Веб-портал в области ГИС и ДЗЗ [Электронный ресурс]. Режим доступа: https://gis-lab.info/
3. Веб-портал в области свободного программного обеспечения [Электронный ресурс]. Режим доступа: http://www.opennet.ru/
4. Веб-портал в области современных технологий [Электронный ресурс]. Режим доступа: https://www.computerra.ru/
5. Информационный портал «ГИС-ассоциация: Межрегиональная общественная организация содействия развитию рынка геоинформационных технологий и услуг» [Электронный ресурс]. Режим доступа: http://www.gisa.ru/
6. Информационный портал «Научная Россия» [Электронный ресурс]. Режим доступа: https://scientificrussia.ru/
7. Сетевое издание «IT-World: Мир цифровых и информационных технологий» [Электронный ресурс]. Режим доступа: https://www.it-world.ru/
8. Справочно-информационный портал «Грамота.ру» [Электронный ресурс]. Режим доступа: https://gramota.ru/
9. Справочно-правовая система «Гарант» [Электронный ресурс]. Режим доступа: https://www.garant.ru/
10. Справочно-правовая система «Консультант плюс» [Электронный ресурс]. Режим доступа: https://www.consultant.ru/

8.5. Перечень профессиональных баз данных

1. База данных исследований Центра стратегических разработок [Электронный ресурс]. Режим доступа: https://www.csr.ru/ru/research/
2. База данных международных индексов научного цитирования Scopus [Электронный ресурс]. Режим доступа: http://www.scopus.com/
3. База данных международных индексов научного цитирования Web of Science [Электронный ресурс]. Режим доступа: http://webofscience.com/
4. База данных НП «Международное Исследовательское Агентство «Евразийский Монитор» [Электронный ресурс]. Режим доступа: https://eurasiamonitor.org/issliedovaniia

5. База книг и публикаций электронной библиотеки «Наука и Техника» [Электронный ресурс]. Режим доступа: https://n-t.ru/

6. Базы данных официальной статистики Федеральной службы государственной статистики [Электронный ресурс]. Режим доступа: https://rosstat.gov.ru/statistic

7. Геопортал данных ДЗЗ Роскосмоса [Электронный ресурс]. Режим доступа: https://gptl.ru/

8. Электронная библиотечная система «Znanium» [Электронный ресурс]. Режим доступа: https://znanium.ru/

9. Электронная библиотечная система «Юрайт» (договор № 189-2024 от 23.12.2024 г.) [Электронный ресурс]. Режим доступа: https://urait.ru/

10. Электронная научная библиотека «Elibrary» [Электронный ресурс]. Режим доступа: https://elibrary.ru/

11. Национальное управления океанических и атмосферных исследований NOAA [Электронный ресурс]. Режим доступа: https://www.iaea.org/

12. ЕСИМО – межведомственная федеральная информационная система. Единая государственная система информации об обстановке в мировом океане [Электронный ресурс]. Режим доступа: https://esimo.ru/

13. Федеральная служба государственной статистики (Профессиональная база данных) [Электронный ресурс]. Режим доступа: http://www.gks.ru/

14. Официальная статистика РФ ЕМИСС [Электронный ресурс]. Режим доступа: https://www.fedstat.ru/

15. Информационно-аналитическая система SCIENCE INDEX

9. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение программы соответствует действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов аудиторных занятий и самостоятельной работы студентов.

Учебная аудитории для проведения занятий лекционного типа — укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитория для групповых и индивидуальных консультаций — укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебная аудитория для текущего контроля и промежуточной аттестации — укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Учебно-научный лабораторный центр «ИНФОГЕО» — укомплектована специализированной (учебной) мебелью, компьютерами, служащими для работы с информацией.

Помещение для самостоятельной работы — укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду организации.

Помещение для хранения и профилактического обслуживания учебного оборудования.

10. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

11. Возможность применения электронного обучения и дистанционных образовательных технологий

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий.

Рассмотрено и рекомендовано к использованию в учебном процессе на 24/25 учебный год без изменений*

Протокол заседания кафедры прикладной информатики от 27.06.2024 №6

Рассмотрено и рекомендовано к использованию в учебном процессе на 25/26 учебный год без изменений*

Протокол заседания кафедры прикладной информатики от 20.06.2025 №6

Рассмотрено и рекомендовано к использованию в учебном процессе на 26/27 учебный год без изменений*

Протокол заседания кафедры прикладной информатики от 11.06.2026 №12

*Заполняется при ежегодном пересмотре программы, если в неё не внесены изменения