Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«17» апреля 2024 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.03 Анализ защищенности сетей**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №42 от «15» апреля 2024 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8 от «8» апреля 2024 г.

И.О. зав. кафедрой _____ Колесник С.Н.

Иркутск 2024 г.

Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Преподавание дисциплины «Анализ защищенности сетей» имеет своей целью:

- обучить основам построения и эксплуатации компьютерных сетей;
- принципам и методам защиты информации в компьютерных сетях;
- навыкам комплексного проектирования, построения, обслуживания и анализа защищенных компьютерных сетей.

Для достижения поставленной цели сформулированы следующие задачи - дать осиновые понятия:

- архитектуры вычислительных сетей;
- программно-аппаратных и технических средств создания сетей;
- принципов построения сетей и управления ими;
- использования программных и аппаратных технологий защиты сетей;
- методологии проектирования и сопровождения безопасных сетей;
- обследования и анализа защищенных компьютерных сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Анализ защищенности сетей» является обязательной дисциплиной из вариативной базовой части дисциплин профессионального цикла. Преподавание дисциплины опирается на знания, полученные в ходе изучения дисциплины «Информатика» и «Безопасность операционных систем», которые должны быть освоены полностью, и студенты должны владеть навыками работы на ПЭВМ в операционной системе Linux.

Дисциплина является предшествующей для таких дисциплин профессионального цикла как «Комплексная система защиты информации», а также для производственной практики и итоговой государственной аттестации. Изучение данной дисциплины позволяет приобрести первичные навыки, необходимые для изучения безопасности автоматизированных систем.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-2 Способен проводить анализ уязвимостей системы защиты информации и автоматизированных систем.	ИДК$_{ПК2.1}$ Проводит анализ уязвимостей системы защиты информации ИДК$_{ПК2.2}$ Проводит анализ уязвимостей автоматизированных систем	Знать: • угрозы и методы нарушения ИБ сетевых АС; • роль человеческого фактора в обеспечении безопасности сетей; • принципы функционирования основных защищенных сетевых протоколов; Уметь: • проводить анализ сетевых АС с точки зрения обеспечения ИБ;

		• применять защищенные протоколы и межсетевые экраны, необходимые для реализации СЗИ в сетях; Владеть: • навыками применения мер противодействия выявленным угрозам сетевой безопасности с использованием различных программно-аппаратных средств защиты в соответствии с правилами их использования.
ПК-3 Способен внедрять организационные меры по защите информации в автоматизированных системах.	$ИДК_{ПК3.1}$ Внедряет организационные меры по защите информации в автоматизированных системах. $ИДК_{ПК3.2}$ Выбирает организационные меры по защите информации в автоматизированных системах.	Знать: • методологические и технологические основы обеспечения информационной безопасности (ИБ) сетевых автоматизированных систем (АС); • методы и средства проектирования, реализации и оценки защищенных сетевых систем;. Уметь: • разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства защиты; • применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации (СЗИ) в АС; • реализовать СЗИ в АС в соответствии со стандартами. Владеть: • навыками оформления рабочей технической документации с учетом действующих нормативных и методических документов

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, 108 часов,
из них 31 час – практическая подготовка обучающихся
Форма промежуточной аттестации: зачет

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Тема 1.	6	23	7	4	8		11	Тестовый контроль по теме
2	Тема 2.	6	24	7	4	8	1	12	Тестовый контроль по теме
3	Тема 3.	6	24	7	4	8		12	Тестовый контроль по теме
4	Тема 4.	6	24	7	4	8		12	Тестовый контроль по теме

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
5	Тема 1	Решение задач, Подготовка тестовых материалов	1-2 неделя	11	Задание №1	Учебный сайт
5	Тема 2	Решение задач, Подготовка тестовых материалов	3-4 неделя	12	Задание №2	Учебный сайт
5	Тема 3	Решение задач, Подготовка тестовых материалов	5-6 неделя	12	Задание №3	Учебный сайт
5	Тема 4	Решение задач, Подготовка тестовых материалов	7-8 неделя	12	Задание №4	Учебный сайт
Общий объем самостоятельной работы по дисциплине (час)				**47**		

4.3. Содержание учебного материала

Тема 1. Введение. Основы организации компьютерных сетей

Предмет, задачи и содержание дисциплины. Цели и задачи организации компьютерных сетей в защищенном исполнении. Вопросы экономичности и эффективности. Постановка задачи распределенной обработки данных; классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. Основы организации и функционирования сетей. Сетевые операционные системы. Основные сетевые стандарты. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиент-сервер. Одноранговые сети.

Тема 2. Безопасность ресурсов сети.

Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Средства повышения надежности функционирования сетей.

Тема 3. Интеграция локальных сетей в региональные и глобальные сети.

Организация сетей на базе операционных систем Unix. Организация компьютерных сетей на базе операционных систем Windows. Организация компьютерных сетей на базе операционных систем Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений. Неоднородные вычислительные сети.

Тема 4. Технологии обеспечения информационной безопасности в глобальной сети Internet.

Основные службы и предоставляемые услуги, основные протоколы, функционирование, разработка и сопровождение приложений, особенности реализации на различных платформах, стандарты. Перспективы развития. Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Языковые средства представления информации в Internet. Организация корпоративных сетей в Internet.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1.	Тема 1	Контрольная работа №1	12	7	Тестовый контроль по теме	ПК-2
2.	Тема 2	Контрольная работа №2	12	7	Тестовый контроль по теме	ПК-2

3.	Тема 3	Контрольная работа №3	12	7	Тестовый контроль по теме	ПК-3
4.	Тема 4	Контрольная работа №4	12	7	Тестовый контроль по теме	ПК-3

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	Тема 1	Решение задач, Подготовка тестовых материалов	ПК-2	ПК-2.1 ПК-2.2
2	Тема 2	Решение задач, Подготовка тестовых материалов	ПК-2	ПК-2.1 ПК-2.2
3	Тема 3	Решение задач, Подготовка тестовых материалов	ПК-3	ПК-3.1 ПК-3.2
4	Тема 4	Решение задач, Подготовка тестовых материалов	ПК-3	ПК-3.2

4.4. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Анализ защищенности сетей», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету и экзамену.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Анализ защищенности сетей», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

4.5. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — ISBN 978-5-9997-0805-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292247 (дата обращения: 01.05.2022). — Режим доступа: для авториз. пользователей.
2. Ларина, Т. Б. Сетевые средства операционных систем : учебное пособие / Т. Б. Ларина. — Москва : РУТ (МИИТ), 2021. — 106 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/269561 (дата обращения: 01.05.2022). — Режим доступа: для авториз. пользователей.

б) дополнительная литература

1. Практикум по администрированию программного обеспечения : учебное пособие / составитель И. В. Анзин. — Ставрополь : СКФУ, 2017. — 85 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155248 (дата обращения: 01.05.2022). — Режим доступа: для авториз. пользователей.

г) базы данных, информационно-справочные и поисковые системы

1. Учебный сайт Лаборатории ТЗИ Физического факультета ИГУ - https://sites.google.com/view/ltzi/, – Режим доступа: свободный.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Компьютерный класс 323Б (12 рабочих мест), оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет.

6.2. Программное обеспечение

Операционная система Альт Сервер компании «Базальт СПО».

6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля

знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для достижения планируемых результатов обучения, в дисциплине «Безопасность операционных систем» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем информационной безопасности, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные средства для входного контроля

Входной контроль (25 вариантов, 3-й семестр), представляет собой перечень из 10-15 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

8.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям. Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

8.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

Тестовые работы. Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Демонстрационный вариант контрольной работы №1

1. Что такое вычислительная сеть (ВС), дайте определение.
2. По каким признакам можно классифицировать ВС?
3. Какие виды ВС Вам известны по уровням?
4. Какие основные сетевые стандарты?
5. Приведите примеры задач, которые можно решать с помощью ВС разных конфигураций.
6. Что такое идентификация и аутентификация, определение.
7. Каковы методы идентификации и аутентификации, их характеристики?
8. Назовите и охарактеризуйте способ повышения надежности функционирования сетей.
9. Назовите и охарактеризуйте средства повышения надежности функционирования сетей.
10. Какие ВС возможно организовать на базе операционных систем Linux?
11. Какие ВС возможно организовать на базе операционных систем Windows.?
12. Назовите основные подсистемы Windows., какие задачи они выполняют?
13. Какие ВС возможно организовать на базе операционных систем Unix?
14. Какова история создания и функционирования Internet?
15. Назовите основные платформы и стандарты функционирования Internet.
16. Каковы основные механизмы обеспечения безопасности информации при применении Internet?
17. Каковы основные способы и средства обеспечения безопасности информации при работе Internet?
18. Особенности обеспечения безопасности при распределении информационных ресурсов в организации.
19. Межсетевые экраны, назначение, порядок применения.
20. Структура и состав МЭ, порядок установки в ВС.
21. Схемы защиты на основе применения МЭ в ВС.
22. Конфигурации ВС с применением МЭ.

Разработчик:

_____	доцент	С.Н. Колесник
(подпись)	(занимаемая должность)	(инициалы, фамилия)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «8» апреля 2024 г. протокол № 8

И.О. зав. кафедрой _____ Колесник С.Н.