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.
«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.ДВ.02.01 Анализ защищенности сетей**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки №4 Безопасность автоматизированных систем (в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

стр.

1. Цели и задачи дисциплины (модуля) 3
2. Место дисциплины в структуре ОПОП 3
3. Требования к результатам освоения дисциплины (модуля) 3
4. Объем дисциплины (модуля) и виды учебной работы 5
5. Содержание дисциплины (модуля) 5
   5.1. Содержание разделов и тем дисциплины (модуля) 5
   5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами 5
   5.3. Разделы и темы дисциплин (модулей) и виды занятий 7
6. Перечень семинарских, практических занятий и лабораторных работ 7
   6.1. План самостоятельной работы студентов 8
   6.2. Методические указания по организации самостоятельной работы студентов 8
7. Примерная тематика курсовых работ (проектов) 9
8. Учебно-методическое и информационное обеспечение дисциплины (модуля): 10
   а) основная литература ..... **Ошибка! Закладка не определена.**
   б) базы данных, информационно-справочные и поисковые системы ..... **Ошибка! Закладка не определена.**
9. Материально-техническое обеспечение дисциплины (модуля) 10
10. Образовательные технологии 10
11. Оценочные средства (ОС): 11
    11.1. Оценочные средства для входного контроля 11
    11.2. Оценочные средства текущего контроля 11
    11.3. Оценочные средства для промежуточной аттестации 12

1. Цели и задачи дисциплины (модуля)

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

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 (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

- способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

В результате изучения дисциплины студент должен:

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.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		6	-	-	-
Аудиторные занятия (всего)	52/ 1,4	52/ 1,4	-	-	-
В том числе:	-	-	-	-	-
Лекции	16/0,4	16/0,4	-	-	-
Практические занятия (ПЗ)	32/0,9	32/0,9	-	-	-
Семинары (С)	-	-	-	-	-
Лабораторные работы (ЛР)	-	-	-	-	-
Контроль самостоятельной работы (КСР)	4/0,11	4/0,11			
Самостоятельная работа (всего)	56/1,6	56/1,6	-	-	-
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	56/1,6	56/1,6			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	52/1,4	52/1,4			
Общая трудоемкость часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля)

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.

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Безопасность компьютерных сетей	1-4
2	Практика по получению первичных профессиональных умений и навыков	1-4
3	Проектно-технологическая практика	1-4

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	4	8			10	22
2.	***Раздел 2***	Тема 2	4	8			20	32
3.	***Раздел 3***	Тема 3	4	8			10	22
4.	***Раздел 4***	Тема 4	4	8			16	28

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	**Раздел 1.**	Практическая работа №1	2	Тестовый контроль по теме	ПК-2
2.	**Раздел 1.**	Практическая работа №2	2	Тестовый контроль по теме	ПК-2
3.	**Раздел 1.**	Практическая работа №3	2	Тестовый контроль по теме	ПК-8
4.	**Раздел 1.**	Практическая работа №4	2	Тестовый контроль по теме	ПК-2
5.	**Раздел 2.**	Практическая работа №5	2	Тестовый контроль по теме	ПК-8
6.	**Раздел 2.**	Практическая работа №6	2	Тестовый контроль по теме	ПК-8
7.	**Раздел 2.**	Практическая работа №7	3	Тестовый контроль по теме	ПК-2
8.	**Раздел 2.**	Практическая работа №8	3	Тестовый	ПК-2

				контроль по теме	
9.	**Раздел 3.**	Практическая работа №9	2	Тестовый контроль по теме	ПК-2
10.	**Раздел 3.**	Практическая работа №10	2	Тестовый контроль по теме	ПК-8
11.	**Раздел 3.**	Практическая работа №11	2	Тестовый контроль по теме	ПК-8
12.	**Раздел 3.**	Практическая работа №12	2	Тестовый контроль по теме	ПК-2
13	**Раздел 4.**	Практическая работа №13	2	Тестовый контроль по теме	ПК-8
14	**Раздел 4.**	Практическая работа №14	2	Тестовый контроль по теме	ПК-2
15	**Раздел 4.**	Практическая работа №15	2	Тестовый контроль по теме	ПК-8
16	**Раздел 4.**	Практическая работа №16	2	Тестовый контроль по теме	ПК-2

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-2**	Подготовка к контрольной работе №1	№1	Учебный сайт	26
8		Контрольная работа №1.		Учебный сайт	
9		Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.		Учебный сайт	
10-16	**3-4**	Подготовка итоговой зачетной работы	№2	Учебный сайт	30
17		Подготовка доклада с презентацией		Учебный сайт	
18		Подведение итогов		Учебный сайт	

6.2. 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).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

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.

9. Материально-техническое обеспечение дисциплины (модуля)

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

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Анализ защищенности сетей» 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 объектно-ориентированного подхода при разработке программного обеспечение на лекциях, 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 ее студенты 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 плановых и внеплановых консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль (6 вариантов, 5-й семестр), представляет собой перечень из 10 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

11.2. Оценочные средства текущего контроля

В течение курса, студенты по мере изучения тем, студенты выполняют различные задания на практических занятиях и лабораторных работах. На последней лабораторной работе в рамках изучаемой темы, студенты получают и выполняют контрольное спецзадание, направленное на закрепление всех знаний, умений и навыков, полученных на предыдущих занятиях. Контрольное спецзадание представляет из себя задачу на настройку и обеспечение безопасности обмена данными посредством почтового сервера и т.п.

Выполняя спецзадание, студент должен продемонстрировать достаточный уровень навыков и знаний, чтобы получить оценку «зачтено» по данному спецзаданию. Спецзадание считается сданным, если студент полностью реализовал все поставленные задачи и доказал работоспособность программы, алгоритма или модуля. Выполнение спецзаданий и их оценка в будущем отражается при прохождении промежуточной аттестации.

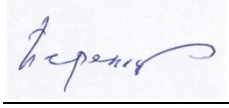
11.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

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.

Разработчики:



_____	доцент	Ю.Н. Переляев
(подпись)	(занимаемая должность)	(инициалы, фамилия)

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой  Колесник С.Н.