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.

«20» апреля 2023 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.34 Программно-аппаратные средства защиты информации**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Техническая защита информации**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №38 от «18» апреля 2023 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 7 от «27» февраля 2023 г.

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

Иркутск 2023 г.

Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Основные цели и задачи, решаемые в ходе преподавания учебной дисциплины, заключаются в формировании у студентов:

- взглядов на защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер;
- понимания базовых теоретические понятий, лежащих в основе процесса защиты информации;
- представления студентам о принципах функционирования и возможностях применения аппаратных средств защиты информации;
- навыков использования программных и программно-аппаратных средств защиты информации.
- высокого профессионализма в работе, чувства ответственности за свой труд, стойких этических навыков.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Программно-аппаратные средства защита информации» базируется на дисциплинах «Математика», «Физика», «Информатика», «Теория информации», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Техническая защита информации», «Дискретная математика», «Электроника и схемотехника», «Электротехника».

Знания, полученные при изучении дисциплины «Программно-аппаратные средства защиты информации» являются необходимыми для успешного освоения следующих дисциплин: «Комплексная система защиты информации», «Основы управления информационной безопасностью», «Организационное и правовое обеспечение информационной безопасности».

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
ОПК-3.2	Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа.	Знать: • основы построения защищенных вычислительных сетей; • основы криптографических преобразований. Уметь: • осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты. Владеть: • навыками выявления угроз

		безопасности автоматизированных систем; • технического обслуживания электронно-вычислительных машин и комплексов; • криптографических и программно-аппаратных средств защиты информации.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетные единицы, 108 часов,
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.	7	9		4	4		5	Тестовый контроль по теме
2	Тема 2.	7	16		4	4		8	Тестовый контроль по теме
3	Тема 3.	7	16		4	4		8	Тестовый контроль по теме
4	Тема 4.	7	17		4	4	1	8	Тестовый контроль по теме

5	Тема 5.	7	16		4	4		8	Тестовый контроль по теме
6	Тема 6	7	20		6	6		8	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.)		
7	Тема 1-3	Подготовка к контрольной работе №1	1-5 неделя	20	Контрольная работа №1	Учебный сайт
7	Тема 1-3	Контрольная работа №1.	6 неделя	2	Контрольная работа №1	Учебный сайт
7	Тема 1-3	Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.	7 неделя	1	Контрольная работа №1	Учебный сайт
7	Тема 4-6	Подготовка к контрольной работе №2	8-11 неделя	19	Контрольная работа №2	Учебный сайт
7	Тема 4-6	Контрольная работа №2.	12 неделя	2	Контрольная работа №2	Учебный сайт
7	Тема 4-6	Подведение итогов по контрольной работе №2. Работа над ошибками по контрольной работе №2.	13 неделя	1	Контрольная работа №2	Учебный сайт
Общий объем самостоятельной работы по дисциплине (час)				**45**		

4.3. Содержание учебного материала

Раздел 1 (Тема 1). ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ.

Основы сетевого и межсетевого взаимодействия. Информационная безопасность. Политика безопасности. Сетевая политика безопасности. Управление рисками. Механизмы и службы защиты.

РАЗДЕЛ 2 (Тема 2). ВРЕДОНОСНЫЕ ПРОГРАММЫ.

Компьютерные вирусы. Файловые вирусы. Макровирусы. Загрузочные вирусы. Методы защиты вирусов от обнаружения. Троянские кони. Сетевые черви. Потайные ходы. Руткиты. Руткиты уровня пользователя. Руткиты уровня ядра. Вредоносные программы для мобильных устройств. Прочие вредоносные программы. Наименование вирусов. Защита от вредоносного программного обеспечения. Технология Black и Whitelisting.

РАЗДЕЛ 3 (Тема 3). УДАЛЕННЫЕ СЕТЕВЫЕ АТАКИ.

Сетевые атаки. Три основных типа атак. Примеры некоторых атак. Классификации удаленных атак. Списки категорий. Матричные схемы. Процессы. Классификация Ховарда. Оценивание степени серьезности атак. .

РАЗДЕЛ 4 (Тема 4). ТЕХНОЛОГИИ МЕЖСЕТЕВЫХ ЭКРАНОВ.

Технологии построения межсетевых экранов. Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояний. Межсетевые экраны уровня ядра. Персональные межсетевые экраны. Распределенные межсетевые экраны. Обход межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Тестирование межсетевых экранов.

Раздел 5 (Тема 5). СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК И ВТОРЖЕНИЙ.

Модели систем обнаружения вторжений. Модель Д. Деннинг. Модель CIDF. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Методы Data Mining. Методы технологии мобильных агентов. Методы построения иммунных систем. Применение генетических алгоритмов. Применение нейронных сетей. Методы обхода систем обнаружения вторжений. Методы обхода хостовых систем обнаружения вторжений. Вспомогательные средства обнаружения. Тестирование систем обнаружения вторжений. Тестирование коммерческих систем. Тестирование исследовательских прототипов. Системы предупреждения вторжений.

Раздел 6 (Тема 6). ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ.

Туннелирование. Протоколы VPN канального уровня. . Протокол IPSec. Ассоциация обеспечения безопасности. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Основные типы защищенных связей. Протоколы VPN транспортного уровня. Цифровые сертификаты. Примеры отечественного построения VPN.

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.	Раздел 1	Лабораторная №1	4		Тестовый контроль по теме	ОПК-3.2
2.	Раздел 2	Лабораторная №2	4		Тестовый контроль по теме	ОПК-3.2
3.	Раздел 3	Лабораторная №3	4		Тестовый контроль по теме	ОПК-3.2
4.	Раздел 4	Лабораторная №4	4		Тестовый контроль по теме	ОПК-3.2
5.	Раздел 5	Лабораторная №5	4		Тестовый контроль по теме	ОПК-3.2
6.	Раздел 6	Лабораторная №6	6		Тестовый контроль по теме	ОПК-3.2

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	Контрольная работа №1.	ОПК-3.2	Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа
2	Тема 2	Контрольная работа №1.	ОПК-3.2	Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа
3	Тема 3	Контрольная	ОПК-3.2	Способен проводить работы по

		работа №1.		установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа
4	Тема 4	Контрольная работа №2.	ОПК-3.2	Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа
5	Тема 5	Контрольная работа №2.	ОПК-3.2	Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа
6	Тема 6	Контрольная работа №2.	ОПК-3.2	Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа

4.4. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Программно-аппаратные средства защиты информации», 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 «Программно-аппаратные средства защиты информации», 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. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 01.05.2023). — Режим доступа: для авториз. пользователей.
2. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 01.05.2023). — Режим доступа: для авториз. пользователей.

б) дополнительная литература

1. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494 (дата обращения: 01.05.2023). — 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:

Компьютерная лаборатория 323б (16 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

6.2. Программное обеспечение

Система тестирования и анализа программно-аппаратной платформы защиты информации.

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 «Программно-аппаратные средства защиты информации» 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, 7-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 тестовой работы

Работа с iptables

Поддержка пакетного фильтра в ядре и сам пакет iptables присутствуют в операционной системе по умолчанию. Поэтому никаких дополнительных настроек не требуется.

Проверка наличия пакета iptables:

[root@SUPERCOMP ~]# apt-cache search iptables | grep iptables

Проверка, что iptables запускается при старте системы:

[root@SUPERCOMP ~]# systemctl status iptables.service

Вывод списка текущих правил iptables:

[root@SUPERCOMP ~]# iptables -L -v

Задание

1. Напишите скрипт для iptables. В этом наборе правил iptables разрешить все исходящие соединения и строго ограничить входящие. Доступ будет возможен по портам TCP: 21, 22, 25, 53, 80, 143, 443, по портам UDP: 20, 21, 53, также пропускаем пакеты для уже установленных соединений.

#!/bin/bash

IPT=”/sbin/iptables”

 # Очищаем правила и удаляем цепочки.

$IPT -F

$IPT -X

 # По умолчанию доступ запрещен.

$IPT -P INPUT DROP

$IPT -P FORWARD DROP

$IPT -P OUTPUT DROP

 # Список разрешенных TCP и UDP портов.

TCP_PORTS=”21,22,25,53,80,143,443”

UDP_PORTS=”53,21,20”

 # Разрешаем пакеты для интерфейса обратной петли.

$IPT -A INPUT -i lo -j ACCEPT

$IPT -A OUTPUT -o lo -j ACCEPT

 # Разрешаем пакеты для установленных соединений.

$IPT -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

 # Разрешаем исходящие соединения.

$IPT -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

 # Разрешаем доступ к портам, описанным в переменных TCP_PORTS

#и UDP_PORTS.

$IPT -A INPUT -p tcp -m multiport --dport $TCP_PORTS -j ACCEPT

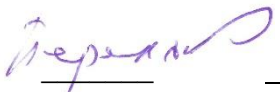
$IPT -A INPUT -p udp -m multiport --dport $UDP_PORTS -j ACCEPT

 # Разрешаем исходящий ping.

$IPT -A INPUT -p icmp -m icmp --icmp-type echo-reply -j ACCEPT

2. Сделайте скрипт исполняемым.
3. Запустите его.
4. Выведите список текущих правил iptables.

Разработчик:



_____ доцент_____ _____Ю.Н.Переляев_____

(подпись) (занимаемая должность) (инициалы, фамилия)

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

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «27» февраля 2023 г. протокол № 7

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