МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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.Б.07 «Программно-аппаратные средства защиты информации»

Направление подготовки 10.03.01 «Информационная безопасность»

Тип образовательной программы: Бакалавриат

Направленность (профиль) подготовки: №7 Техническая защита информации

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)

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

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 (модуля)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общепрофессиональные компетенции (ОПК):

ОПК-7 *способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты*

В результате изучения дисциплины студент должен:

***Знать**:*

Индекс компетенции	*Образовательный результат*
ОПК-7	*основы построения защищенных вычислительных сетей;*
	основы криптографических преобразований.

***Уметь**:*

Индекс компетенции	*Образовательный результат*

ОПК-7	• осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.

Владеть:

Индекс компетенции	*Образовательный результат*
ОПК-7	*навыками выявления угроз безопасности автоматизированных систем;*
	технического обслуживания электронно-вычислительных машин и комплексов;

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		7			
Аудиторные занятия (всего)	54/1,5	54/1,5			
В том числе:			-	-	-
Лекции	26/0,7	26/0,7	-	-	-
Практические занятия (ПЗ)			-	-	-
Семинары (С)			-	-	-
Лабораторные работы (ЛР)	26/0,7	26/0,7	-	-	-
Контроль самостоятельной работы (КСР)	2/0,05	2/0,05			
Самостоятельная работа (всего)	54/1,5	54/1,5	-		
В том числе:			-	-	-
Курсовой проект (работа)			-	-	-
Расчетно-графические работы	-	-	-		
Реферат (при наличии)	-	-	-	-	-
Другие виды самостоятельной работы	54/1,5	54/1,5	-	-	-
Вид промежуточной аттестации (*зачет*)	зачет	зачет			
Контактная работа (всего)	54/1,5	54/1,5			
Общая трудоемкость, часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

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.

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

№ п/п	Наименование обеспечиваемых (последующих)	№№ разделов и тем данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин

	дисциплин						
		1	2	3	4	5	6
1	Базы данных	+	+	+	+	+	+
2	Теория информации	+	+	+	+	+	+
3	Объектно-ориентированное программирование	+	+	+	+	+	+

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	Тема 1.	Тема 1.	4			4	9	17
2	Тема 2.	Тема 2.	4			4	9	17
3	Тема 3.	Тема 3.	4			4	9	17
4	Тема 4.	Тема 4.	4			4	9	17
5	Тема 5.	Тема 5.	6			6	9	21
6	Тема 6	Тема 6	4			4	9	17

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	Лабораторная №1	4	Решение заданий на лабораторных работах. Домашняя работа	*ОПК-7*
2	Раздел 2	Лабораторная №2	4	Решение заданий на лабораторных работах. Домашняя работа	*ОПК-7*
3	Раздел 3	Лабораторная №3	4	Решение заданий на лабораторных работах. Домашняя работа	*ОПК-7*
4	Раздел 4	Лабораторная №4	4	Решение заданий на	*ОПК-7*

				лабораторных работах. Домашняя работа	
5	Раздел 5	Лабораторная №5	6	Решение заданий на лабораторных работах. Домашняя работа	*ОПК-7*
6	Раздел 6	Лабораторная №6	4	Решение заданий на лабораторных работах. Домашняя работа	*ОПК-7*

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Тема 1-3	Подготовка к контрольной работе №1	Анализ лекционного материала, изучение литературы.	Источники из основной и дополнительной литературы по теме практических занятий. Образовательные ресурсы, доступные по логину и паролю, предоставляемым Научной библиотекой	9
1	Тема 1-3	Контрольная работа №1.	Разбор задач аналогичных лекционным и лабораторным		9
2	Тема 1-3	Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.	Разбор задач аналогичных лекционным и лабораторным		9
3	Тема 4-6	Подготовка к контрольной работе №2	Разбор задач аналогичных лекционным и лабораторным		9
4	Тема 4-6	Контрольная работа №2.	Разбор задач аналогичных лекционным и лабораторным		9

5	Тема 4-6	Подведение итогов по контрольной работе №2. Работа над ошибками по контрольной работе №2.	Разбор задач аналогичных лекционным и лабораторным		9
6	Тема 1-3	Домашняя работа	Разбор задач аналогичных лекционным и лабораторным		9

6.2. 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).

7. Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрено написание курсовых проектов

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

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.
3. 3. 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.

б) 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):

Для проведения занятий лекционного типа в качестве демонстрационного оборудования используется меловая доска, проектор, ноутбук. Наглядность обеспечивается путем изображения схем, диаграмм и формул с помощью мела. Использование глобальной компьютерной сети позволяет обеспечить доступность Интернет-ресурсов и реализовать самостоятельную работу студентов.

На факультете имеется компьютеризированная аудитория, предназначенная для лабораторной работы, а также аудитория для самостоятельной работы, с неограниченным доступом в Интернет.

Материалы: учебно-методические пособия, контрольные задания для аудиторной и самостоятельной работы студентов.

10. Образовательные технологии:

Задачи изложения и изучения дисциплины реализуются в следующих формах деятельности:

- лекции, нацеленные на получение необходимой информации, и ее использование при решении практических/лабораторных задач;
- лабораторные занятия, направленные на активизацию познавательной деятельности студентов и приобретения ими навыков решения практических и проблемных задач;
- консультации – еженедельно для всех желающих студентов;
- самостоятельная внеаудиторная работа направлена на приобретение навыков самостоятельного решения задач по дисциплине;
- текущий контроль за деятельностью студентов осуществляется на лекционных и лабораторных занятиях в ходе самостоятельного решения задач.

11. Оценочные средства (ОС):

11.1. 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.

11.2. Оценочные средства текущего контроля.

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

11.3. Оценочные средства для промежуточной аттестации (в форме зачета).

Материалы для проведения текущего и промежуточного контроля знаний студентов:

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Решение задач на лабораторных занятиях	1-6	ОПК-7

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

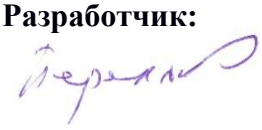
Задание

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_____

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

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