

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

02.02.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.32 Методы и средства создания угроз информационной безопасности

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность) 10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника Специалист
(бакалавр/магистр/специалист)

Специализация Анализ безопасности информационных систем

Курс 4
Семестр 7

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	18	часов
Лабораторные работы	54	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	72	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	72	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	7	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

доцент с ученой степенью кандидата наук	ИБ	СОГЛАСОВАНО	А.А. Кречетов
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационной безопасности

		(наименование кафедры)	
17.01.2022	протокол №	4	
(дата)			
Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина	
		(И.О. Фамилия)	

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)
кафедрой(ами).
СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит
выпускающая кафедра

СОГЛАСОВАНО	А.А. Кречетов
	(И.О. Фамилия)

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 07.02.2022 г.
Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1 знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера	знания: - основы работы в Linux - основные утилиты реализующие тестирование систем на проникновение умения: навыки:
	ОПК-2.2 умеет составлять документы, используя прикладные программы офисного назначения	знания: умения: - составлять грамотные отчеты по результатам тестов на проникновение навыки:
	ОПК-2.3 Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации	знания: - основы работы в Linux - основные утилиты реализующие тестирование систем на проникновение умения: - составлять грамотные отчеты по результатам тестов на проникновение навыки: - разработки программ анализа систем на проникновение

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-2)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические и лабораторные занятия, процедуры самообучения

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Тестирование на проникновение	144	ОПК-2
Лекция. Основы Kali Linux	2	

Лекция. Основы тестирования сетевой безопасности	2
Лекция. Разведка	2
Лекция. Поиск уязвимостей	2
Лекция. Автоматизированные эксплойты	2
Лекция. Владение Metasploit	2
Лекция. Тестирование безопасности беспроводной сети	2
Лекция. Тестирование веб-приложений	2
Лекция. Взлом паролей	2
Лабораторная работа. Поиск уязвимостей	10
Лабораторная работа. Автоматизированные эксплойты	12
Лабораторная работа. Тестирование безопасности беспроводной сети	12
Лабораторная работа. Тестирование веб-приложений	10
Лабораторная работа. Взлом паролей	10
Задания для самостоятельной работы, в том числе выполнение Проработка лекций	
Подготовка к выполнению лабораторных работ	72
Иная контактная работа: дифференцированный зачет (БРК)	0

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины (**модуля**) рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности. **Занятия лекционного типа** дают систематизированные знания по дисциплине (**модулю**), концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. (**при наличии**) Содержание **самостоятельной работы** определяется рабочей программой дисциплины (**модуля**), оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины (**модуля**), к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Изучение дисциплины (**модуля**) включает выполнение **лабораторной работы**. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине (**модулю**) является **балльно-рейтинговый контроль**.

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющихся в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Колисниченко, Денис Николаевич. Linux. От новичка к профессионалу [Текст] : [наиболее полное руководство] / Денис Колисниченко. 4-е изд. Санкт-Петербург: БХВ-Петербург, 2012. - 690 с. ISBN 978-5-9775-0824-7. Экземпляры: всего 5.	5
2.	Linux Устранение неполадок [Текст] / Джеймс Киркланд [и др.] ; [пер. с англ. А. А. Слинкин]. Москва: НТ Пресс, 2009. - 490 с. ISBN 978-5-477-00574-1. Экземпляры: всего 5.	5
3.	Немет, Эви. Руководство администратора Linux [Текст] / Эви Немет, Гарт Снайдер, Трент Р. Хейн при участии Линды Мак-Гинли [и др. ; пер. с англ. Я. П. Волковой и др.]. 2-е изд. Москва: Вильямс, 2011. - 1071 с. ISBN 978-5-8459-1093-6. Экземпляры: всего 5.	5
4.	Блам, Р. Администрирование почтовых серверов sendmail [Электронный ресурс] / Блам Р. 2-е изд. Москва: ИНТУИТ, 2016. - 702 с. ISBN 5-9570-0037-X.	https://e.lanbook.com/book/100558
5.	Гончарук, С. В. Администрирование ОС Linux [Электронный ресурс] / Гончарук С. В. 2-е изд. Москва: ИНТУИТ, 2016. - 164 с.	https://e.lanbook.com/book/100568

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	107 (III)	Анализатор линейных коммуникаций УЛАН-2 (1), Генератор шума Соната -P2 (1), Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Коммутатор D-Link DES-3200-28 (8), Коммутатор D-Link DES-3810-28 (2), Комплекс защиты информации Secret Disk 4.0 (1), Комплекс защиты информации Secret Net 5.0 (2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Нелинейный локатор SEL SP-61/M "Катран" (1), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ	Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ПО для решения основных пользовательских задач

		G2450NM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450NM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Система виброакустической защиты "Соната-AB" (1), Система виброакустической.защиты "Соната-PC2" (1), Средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е" (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	
--	--	--	--

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними	отлично

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

1. Угроза безопасности компьютерной системы – это

- а) потенциально возможное происшествие, которое может оказать нежелательное воздействие на систему и хранящуюся в ней информацию
- б) некая неудачная характеристика системы
- в) действие, которое заключается в поиске и использовании какой-либо уязвимости
- г) все выше перечисленные

2. На каком уровне модели OSI может осуществляться атака

- а) транспортном и физическом
- б) представительном и канальном
- в) физическом и канальном
- г) на всех

3. Подмена доверенного объекта PBC – это

- а) пассивное воздействие с целью нарушения конфиденциальности
- б) активное воздействие с целью нарушения конфиденциальности
- в) пассивное воздействие с целью нарушения работоспособности
- г) активное воздействие с целью нарушения работоспособности

4. Протокол Telnet пересылает пароль

- а) посимвольно (один символ в одном пакете)
- б) весь пароль в одном пакете
- в) а и б
- г) не знаю

5. Методом открытого сканирования является

- а) атака по FTP
- б) сканирование через прокси-сервер
- в) сканирование TCP SYN
- г) сканирование с использованием «немного» хоста

6. Укажите протокол, принадлежащий семейству TCP/IP

- а) RDP
- б) UDP
- в) ICMP
- г) все выше перечисленные

7. Удаленная атака может начаться

- а) по запросу от атакуемого объекта
- б) при наступлении ожидаемого события на атакуемом объекте
- в) по желанию атакующего
- г) все выше перечисленное

8. Навязывание объекту RBC ложного маршрута – это

- а) пассивное воздействие с целью нарушения конфиденциальности
- б) активное воздействие, безусловное к цели атаки
- в) активное воздействие с целью нарушения конфиденциальности
- г) пассивное воздействие, безусловное к цели атаки

9. Для передачи DNS-запрос используется протокол

- а) TCP
- б) UDP
- в) IP
- г) а и б

10. Методом «невидимого» сканирования является

- а) сканирование TCP FIN
- б) сканирование через прокси-сервер
- в) сканирование TAP IDENT
- г) сканирование с использованием IP-фрагментации

Перечень вопросов для проведения промежуточной аттестации

1. Протоколы и адресация в Internet.
2. Служба имен доменов Internet.
3. Классификация удаленных атак на РВС.
4. Понятие типовой удаленной атаки. Анализ сетевого трафика.
5. Понятие типовой удаленной атаки. Подмена доверенного объекта или субъекта РВС.
6. Понятие типовой удаленной атаки. Ложный объект РВС.
7. Понятие типовой удаленной атаки. Отказ в обслуживании.
8. Ложный ARP-сервер в сети Internet.
9. Ложный DNS-сервер в сети Internet.
10. Навязывание ложного маршрута с использованием протокола ICMP.
11. Подмена субъектов TCP-соединения.
12. Атака на rsh-сервер.
13. «Шторм» ложных TCP-запросов.
14. Причины успеха удаленных атак на РВС.
15. Причины успеха удаленных атак на Internet.