

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.1.1.26 Безопасность вычислительных сетей

(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 3
Семестр 5, 6

Распределение учебного времени

Трудоемкость по учебному плану	360 / 10	часов/зачетных единиц
Лекции	72	часов
Лабораторные работы	90	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	162	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	162	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	6	семестр
Зачет	5	семестр
БРК, ДЗ	-	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

31.01.2022	протокол №	23	(наименование кафедры)
(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 /М.Л. Бойкова/

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-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	знания: -основные протоколы, используемые для защиты информации в вычислительных сетях; -основные криптографические методы, используемые для защиты информации в вычислительных сетях; -принципы построения и функционирования локальных и глобальных вычислительных сетей умения: -проводить анализ угроз безопасности в локальных вычислительных сетях; - реализовывать политику безопасности в локальной вычислительной сети навыки: - использование анализатора пакетов с помощью Wireshark
	ОПК-10.2 Обоснование необходимости использования криптографических средств защиты информации	знания: -основные протоколы, используемые для защиты информации в вычислительных сетях; -основные криптографические методы, используемые для защиты информации в вычислительных сетях; -принципы построения и функционирования локальных и глобальных вычислительных сетей умения: -проводить анализ угроз безопасности в локальных вычислительных сетях; - реализовывать политику безопасности в локальной вычислительной сети навыки: - использование анализатора пакетов с помощью Wireshark
	ОПК-10.3 владеет навыками применения инструментальных средств анализа безопасности программного обеспечения при построении систем защиты информации автоматизированных систем	знания: умения: навыки: - использование анализатора пакетов с помощью Wireshark

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 дисциплинах: Методы и средства криптографической защиты информации (ОПК-10); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-10)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

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

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

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

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Модель ISO/OSI. Поток.	108	ОПК-10
Лекция. Тема 1. Транспортная подсистема вычислительных сетей. Транспортный уровень построения вычислительных сетей. Транспортные протоколы в Internet: TCP и UDP. Интерфейс Berkley Sockets. Угрозы безопасности и средства организации безопасного информационного взаимодействия в сетях TCP/IP.	9	
Лекция. Тема 2. Уровень приложений. Представительский и прикладной уровни построения вычислительных сетей. Протоколы прикладного и представительского уровней сети Internet. Система DNS. Администрирование служб доменных имен.	9	
Лабораторная работа. Лабораторная работа 1. Построение элементов структурированной кабельной системы.	18	
Лабораторная работа. Лабораторная работа 2. Построение сетей с помощью коммутаторов. Применение технологии VLAN.	18	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций Подготовка к лабораторным работам	54	
Иная контактная работа: зачет	0	

6 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Безопасность вычислительных сетей	216	ОПК-10
Лекция. Тема 3. Службы локальных вычислительных сетей. Модель «клиент-сервер». Виды серверов и протоколы взаимодействия (HTTP, FTP, SMTP, RDP, SSH и другие). Основные сетевые службы прикладного уровня. Службы файлового обмена. Службы веб-серверов и электронной почты. Служба каталогов Active Directory. Политика безопасности и групповые политики. Решение задач администрирования Active	9	

Directory на базе ОС Windows Server. Решение задач администрирования Active Directory на базе ОС Windows Server. Решение задач администрирования веб-сервера, служб файлового обмена, сервера электронной почты, сервера баз данных.	
Лекция. Тема 4. Алгоритмы криптографической защиты информации в ЛВС. Основные криптографические методы, используемые для защиты информации в вычислительных сетях. Понятие аутентификации. Виды аутентификации. Виды шифрования. Основные протоколы, используемые для защиты информации в вычислительных сетях. Протоколы аутентификации и шифрования с открытым ключом. Организация защищенного канала связи с использованием криптографических протоколов. Виртуальные частные сети. Протокол SSL.	9
Лекция. Тема 5. Анализ защищенности ЛВС. Методы и средства защиты информации в локальных вычислительных сетях. Понятие сетевая атака. Классификация сетевых атак. Виды сетевых атак и методы их реализации. Анализ защищенности и угроз безопасности ЛВС. Сетевое сканирование. Администрирование средств сетевого сканирования и реализации сетевых атак.	9
Лекция. Тема 6. Средства контроля сетевого трафика в ЛВС. Политика безопасности в локальной вычислительной сети. Понятие межсетевого экрана (МСЭ). Функции МСЭ. Классификация МСЭ. Способы реализации МСЭ. Модуль IPTables как средство реализации МСЭ. Настройка IPTables для решения задач фильтрации и блокирования сетевого трафика. Средства контроля доступа к сетевым службам.	9
Лекция. Тема 7. Средства обнаружения вторжений в ЛВС. Классификация средств обнаружения вторжений (СОВ). Способы реализации СОВ. Сетевой анализатор Wireshark. Анализ сетевого трафика и угроз безопасности в ЛВС. Современные программно-аппаратные СОВ. Средства обеспечения безопасности внешнего периметра ЛВС (на примере модуля SNORT).	9
Лекция. Тема 8. Безопасность в ЛВС. Особенности эксплуатации локальных вычислительных сетей с учетом требований по обеспечению безопасности. Средства организации ложного информационного ресурса в ЛВС. Использование средств защиты информации в ЛВС с учетом требований по обеспечению безопасности. Защита информации в ЛВС на разных уровнях: физическом, канальном, сетевом, прикладном. Средства обнаружения несанкционированного доступа к информации на разных уровнях ЛВС. Администрирование ЛВС с учетом требований по обеспечению безопасности.	9
Лабораторная работа. Лабораторная работа 3. Анализ протоколов взаимодействия клиент-серверного приложения с использованием сокетов.	14
Лабораторная работа. Лабораторная работа 4. Применение	14

протокола SNMP.		
Лабораторная работа. Лабораторная работа 5. Организация VPN.	14	
Лабораторная работа. Лабораторная работа 6. Конфигурирование средств обнаружения вторжений.	12	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций		
Подготовка к лабораторным работам	108	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

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. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине (**модулю**) является **зачёт, экзамен**.

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

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Олифер, Виктор Григорьевич. Компьютерные сети [Текст] : принципы, технологии, протоколы : [учебное пособие для студентов вузов по направлению "Информатика и вычислительная техника" и специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных	10

	систем"] / В. Олифер, Н. Олифер. 4-е изд. Санкт-Петербург: Питер, 2014. - 943 с. ISBN 978-5-496-00004-8. Экземпляры: всего 10.	
2.	Олифер, В. Г. Основы сетей передачи данных [Электронный ресурс] / Олифер В. Г., Олифер Н. А. 2-е изд. Москва: ИНТУИТ, 2016. - 219 с.	https://e.lanbook.com/book/100346
3.	Безопасность сетей [Электронный ресурс]. 2-е изд. Москва: ИНТУИТ, 2016. - 571 с. ISBN 5-9570-0046-9.	https://e.lanbook.com/book/100581
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru
2.	Информационно-правовой портал Гарант	http://www.garant.ru

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/М "Катран" (1), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ G2450HM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450HM,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	Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ПО для решения основных пользовательских задач

	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 навыками, приемами выполнения практических работ	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 Сколько уровней в эталонной модели OSI?

а) 4;б) 5;в) 6;г) 7 +

2 Сколько уровней взаимодействия в стеке протоколов TCP/IP?

а) 4; +б) 5;в) 6;г) 7

3 Какие протоколы безопасной аутентификации используются в WLAN-сетях(выберите все возможные варианты)?

а) wep; +б) eap;+в) wpa;+г) eas.

4 Какой протокол отвечает за определение и назначение IP-адреса?:

а) DHCP;

б) DNS;

в) ARP;+

г) IP;

д) TCP

5 Какой протокол отвечает за гарантированную доставку пакета?:

а) DHCP;б) DNS; +в) ARP;г) IP;д) TCP

6 Какой протокол отвечает за определение MAC-адреса?:

а) DHCP;б) DNS;в) ARP;+г) IP;д) TCP

Перечень вопросов для проведения промежуточной аттестации

Вопросы к зачету

1. Примером какого уязвимого места является в NFS установка разрешений корневой директории gw для всех пользователей?
2. Когда используются нетехнические средства для получения доступа в систему?
3. Какая часть памяти является объектом атаки на переполнение буфера?
4. Какой тип переменных используется при выполнении атаки на переполнение буфера?
5. Какая ошибка программирования позволяет выполнить атаку имитации IP-адреса?
6. Какой пакет не отправляется при выполнении синхронной атаки?
7. Существует ли способ защиты от грамотно разработанной DOS-атаки?
8. Что ищут хакеры, использующие ненаправленные методы атак?
9. Как хакер использует систему после взлома с помощью ненаправленной атаки?

10. Какой сайт используется для сбора информации об IP-адресах?
11. Какая часть предварительного исследования является наиболее опасной для хакера при подготовке направленной атаки?
12. Какой тип инструмента представляет собой программа Nmap?
13. С какой целью запускается атака DoS во время выполнения атаки имитации IP-адреса?
14. Чем представляется программа "троянский конь" для пользователя?
15. Для чего нужна программа ps?
16. Перечислите основные службы безопасности.
17. Какая служба полагается на службу конфиденциальности для обеспечения полной защиты информации?
18. Какие службы используются для противостояния атакам на модификацию?
19. В работе каких служб используется система контроля доступа?
20. Должны ли коммерческие организации соблюдать конфиденциальность потока данных?

Вопросы к экзамену

1. Примером какого уязвимого места является в NFS установка разрешений корневой директории gw для всех пользователей?
2. Когда используются нетехнические средства для получения доступа в систему?
3. Какая часть памяти является объектом атаки на переполнение буфера?
4. Какой тип переменных используется при выполнении атаки на переполнение буфера?
5. Какая ошибка программирования позволяет выполнить атаку имитации IP-адреса?
6. Какой пакет не отправляется при выполнении синхронной атаки?
7. Существует ли способ защиты от грамотно разработанной DOS-атаки?
8. Что ищут хакеры, использующие ненаправленные методы атак?
9. Как хакер использует систему после взлома с помощью ненаправленной атаки?
10. Какой сайт используется для сбора информации об IP-адресах?
11. Какая часть предварительного исследования является наиболее опасной для хакера при подготовке направленной атаки?
12. Какой тип инструмента представляет собой программа Nmap?
13. С какой целью запускается атака DoS во время выполнения атаки имитации IP-адреса?
14. Чем представляется программа "троянский конь" для пользователя?
15. Для чего нужна программа ps?
16. Перечислите основные службы безопасности.
17. Какая служба полагается на службу конфиденциальности для обеспечения полной защиты информации?

18. Какие службы используются для противостояния атакам на модификацию?
19. В работе каких служб используется система контроля доступа?
20. Должны ли коммерческие организации соблюдать конфиденциальность потока данных?
21. Какой основной механизм обеспечивает конфиденциальность и целостность информации при передаче?
22. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности?
23. Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
24. Назовите три типа аутентификационных факторов.
25. Почему двухфакторная аутентификация сильнее, чем однофакторная?
26. Зачем нужен аудит?
27. Какие службы позволяют предотвратить атаки на отказ от обязательств?
28. Какие службы позволяют предотвратить атаки доступа?
29. На какие три службы безопасности должен опираться аудит?
30. Примером работы какой службы безопасности является развертывание плана аварийного восстановления?
31. Назовите три раздела, которые должны присутствовать в каждой политике или процедуре.
32. Что определяет политика безопасности?
33. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики?
34. Почему в политику безопасности включают отказы от защиты?
35. Что должна определять политика использования компьютеров?
36. Рекомендуются ли разрешать неограниченное использование компьютеров?
37. Для каких лиц должны указываться требования, содержащиеся в процедурах управления пользователями?
38. Когда сотрудник переходит с одной должности на другую внутри организации, кто должен нести ответственность за уведомление системных администраторов о необходимости изменения профиля доступа данного сотрудника?
39. Какова цель процедуры системного администрирования?
40. Почему необходимо соблюдать внимательность при определении целей IRP?
41. Назовите пять подразделений, сотрудники которых всегда должны входить в группу обработки инцидентов.
42. Назовите четыре ключевых раздела методологии разработки.
43. Назовите три типа событий, которые должны быть указаны в DRP.
44. Какие действия должен выполнять отдел безопасности в процессе создания политики?

45. Почему отдел безопасности должен работать совместно с отделом аудита?
46. Назовите две составляющих риска.
47. Каков уровень риска при отсутствии угроз?
48. Что такое уязвимость?
49. Назовите четыре цели для угроз.
50. Может ли угроза иметь более одной цели?
51. Какими характеристиками должен обладать агент, чтобы представлять собой угрозу?
52. Должен ли агент иметь физический доступ к системе, чтобы представлять собой угрозу?
53. Для какого типа организаций общественность рассматривается как угроза?
54. Только злонамеренные события являются угрозой?
55. После выявления уязвимых мест и угрозы что еще определяется для оценки риска в организации?
56. Назовите пять областей, которые нужно исследовать при оценке риска в организации.
57. С чего начинается определение реальных уязвимых мест?
58. Какая модель используется, если определение особых видов угроз является проблематичным?
59. Можно ли предположить, что большинство организаций в состоянии определить финансовые потери от различного рода инцидентов?
60. Какие затраты сложнее всего измерить?