МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Волгоградский государственный технический университет»

Факультет электроники и вычислительной техники

УТВЕРЖДЕНО
Факультет электроники и вычислительной техники
Декан Авдеюк О.А.
г.

Защита информации

рабочая программа дисциплины (модуля, практики)

Закреплена за кафедрой **Электронно-вычислительные машины и системы**

Учебный план Направление 09.03.04 Программная инженерия

Профиль **Разработка программно-информационных систем**

Квалификация **бакалавр**

Срок обучения **4 года**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Виды контроля в семестрах: экзамены 7

Семестр(Курс.Номер семестра на курсе)	**7(4.1)**		Итого	
	УП	ПП	УП	ПП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64.35	64.35	64.35	64.35
Сам. работа	116	79.65	116	79.65
Часы на контроль	35.65	0	35.65	0
Практическая подготовка	0	0	0	0
Итого трудоемкость в часах	216	144	0	0

ЛИСТ ОДОБРЕНИЯ, СОГЛАСОВАНИЯ И АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

Разработчик(и) программы:

доцент Быков Дмитрий Владимирович ктн

Рецензент(ы):
(при наличии)

Рабочая программа дисциплины (модуля, практики)
Защита информации

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.04 Программная инженерия (приказ Минобрнауки России от 19.09.2017 г. № 920)

составлена на основании учебного плана:
Направление 09.03.04 Программная инженерия

Профиль: Разработка программно-информационных систем

утвержденного учёным советом вуза от 05.06.2019 протокол № 12.

Рабочая программа одобрена на заседании кафедры
Электронно-вычислительные машины и системы

номер протокола 2019 г.
Зав. кафедрой Андреев Андрей Евгеньевич

СОГЛАСОВАНО:
Факультет электроники и вычислительной техники
Председатель НМС факультета: Авдеюк О.А.

Протокол заседания НМС от
г. №

Рабочая программа дисциплины (модуля, практики) актуализирована 31.08.2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ). ВИД, ТИП ПРАКТИКИ, СПОСОБ И ФОРМА (ФОРМЫ) ЕЕ ПРОВЕДЕНИЯ.
Изучение принципов, методов и способов организации информационной безопасности в компьютерах, вычислительных системах, комплексах, локальных, корпоративных, глобальных сетях, протоколах передачи, обработки, хранения информации.
Задачи изучения дисциплины
• формирование теоретических и практических навыков и знаний об особенностях ассиметричных и симметричных алгоритмов;
• изучение технологий электронной подписи;
• рассмотрение основ построения инфраструктуры открытых ключей
• изучение основ информационной безопасности в компьютерных сетях и операционных системах.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Теория вероятностей и математическая статистика
2.1.3	Сети и телекоммуникации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Аппаратно-программные средства компьютерных сетей
2.2.3	Администрирование, сопровождение и DevOps
2.2.4	Производственная практика: Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ОПК-3.1: Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
Результаты обучения: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.2: Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
Результаты обучения: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3.3: Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности
Результаты обучения: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Форма контроля
1	**Раздел 1. Обучение**			
1.1	Вводная лекция /Тема/	7	0	
1.1.1	Основные понятия и определения, источники, риски и формы атак на информацию, политика безопасно-сти /Лек/	7	2	Экз, Кр
1.1.2	Стандарты безопасности /Ср/	7	2	Экз, Кр
1.2	Домашинные методы шифрования /Тема/	7	0	
1.2.1	Шифры замены и перестановки. Шифр Цезаря. Шифр Полибия. Афинная криптосистема. Методы вскрытия одноалфавитных систем. Мнгоалфавитные системы. Шифр Вернама. Шифр Вижинера. Шифр с автоключом. Перестанвочный шифр с ключевым словом. /Лек/	7	2	Экз, Кр

1.2.2	Шифровальная машина Энигма /Ср/	7	2	Экз, Кр
1.2.3	Домешанные методы шифрования /Лаб/	7	4	Экз, Кр
1.3	Блочные симметричные шифры /Тема/	7	0	
1.3.1	Описание симметричных систем шифрования. Схема Фейстеля. Режимы работы блочных шифров. /Лек/	7	2	Экз, Кр
1.3.2	Виды современных симметричных алгоритмов /Ср/	7	2	Экз, Кр
1.4	Примеры симметричных блочных алгоритмов шифрования /Тема/	7	0	
1.4.1	ГОСТ 28147-89. Основной шаг алгоритма. Циклы алгоритма. Ре-жимы алгоритма. DES – общее описание и алгоритм работы типо-вого этапа. /Лек/	7	2	Экз, Кр
1.4.2	Распараллеливание блочных алгоритмов шифрования /Лаб/	7	4	Экз, Кр
1.4.3	Алгоритм AES /Ср/	7	2	Экз, Кр
1.5	Потоковые шифры /Тема/	7	0	
1.5.1	Принципы работы потоковых систем шифрования. Самосинхронизирующиеся потоковые шифры. Синхронные потоковые шифры. /Лек/	7	2	Экз, Кр
1.5.2	Реализация потоковых шифров в режимах блочного шифрования /Ср/	7	2	Экз, Кр
1.6	Системы шифрования с асимметричными открытыми ключами /Тема/	7	0	
1.6.1	Особенности реализации и требова-ния к ассиметричным алгоритмам. Пример работы асимметричного шифрования. Схема цифрового конверта. Алгоритм RSA /Лек/	7	2	Экз, Кр
1.6.2	Алгоритм Эль-Гамаля /Ср/	7	2	Экз, Кр
1.7	Контроль целостности информации /Тема/	7	0	
1.7.1	Криптографические методы контроля целостности. Обнаружение манипуляций с данными. /Лек/	7	2	Экз, Кр
1.7.2	Алгоритмы контроля целостности /Ср/	7	2	Экз, Кр
1.8	Однонаправленные алгоритмы /Тема/	7	0	
1.8.1	Хеш-функции. Стандарты хеширования и протоколы электронной подписи. Алгоритмы аутентификации пользователей. /Лек/	7	2	Экз, Кр
1.8.2	Распараллеливание алгоритмов хэш-функций /Лаб/	7	4	Экз, Кр
1.8.3	Алгоритмы md5, sha256 /Ср/	7	2	Экз, Кр
1.9	Электронная подпись /Тема/	7	0	
1.9.1	Необходимость применения электронной подписи. Общий алгоритм выполнения и проверки электронной подписи /Лек/	7	2	Экз, Кр
1.9.2	Алгоритм DSA /Ср/	7	2	Экз, Кр
1.10	Уязвимость асимметричных криптосистем /Тема/	7	0	
1.10.1	Атака «человек посередине». Варианты устранения уязвимости асимметричных криптосистем. /Лек/	7	2	Экз, Кр
1.10.2	Другие атаки на асимметричные системы /Ср/	7	4	Экз, Кр
1.11	Сертификация открытого ключа /Тема/	7	0	
1.11.1	Понятие и смысл сертификата открытого ключа. Стандарт x509. Струткура сретификата по стандар-ту x509. Отзыв сертификатов. /Лек/	7	2	Экз, Кр
1.11.2	Варианты отзыва сертификата /Ср/	7	2	Экз, Кр
1.11.3	Защиты электронной почты /Лаб/	7	4	
1.12	Инфраструктура открытых ключей /Тема/	7	0	
1.12.1	Организация инфраструктуры открытых ключей. Понятие Удостоверяющего центра. Основные ком-поненты удостоверяющего центра. /Лек/	7	2	Экз, Кр
1.12.2	Разворачивание УЦ на базе MS CA /Лаб/	7	8	
1.12.3	Назначение компонент УЦ /Ср/	7	4	
1.13	Удостоверяющий центр /Тема/	7	0	
1.13.1	Жизненный цикл ключей и сертификатов. Режимы работы удостоверяющего центра. /Лек/	7	2	Экз, Кр
1.13.2	Работа КриптоПро УЦ /Ср/	7	4	Экз, Кр
1.14	Модели доверия удостоверяющих центров /Тема/	7	0	
1.14.1	Иерархическая модель доверия. Сетевая модель доверия. Мостовая модель доверия. /Лек/	7	2	Экз, Кр
1.14.2	Другие виды моделей доверия /Ср/	7	2	Экз, Кр

1.15	Протоколы аутентификации /Тема/	7	0	
1.15.1	Варианты организации аутентификации. Парольная, криптографическая, биометрическая аутентификация. /Лек/	7	2	Экз, Кр
1.15.2	Аутентификация Kerberos /Ср/	7	2	
1.16	Криптографическая защита информации в ОС Windows /Тема/	7	0	
1.16.1	Интерфейс CryptoAPI. Криптопровайдеры. Протокол IPSec. /Лек/	7	2	Экз, Кр
1.16.2	Криптопровайдепы в *nix /Ср/	7	2	Экз, Кр
1.16.3	Реализация приложений с использованием CryptoAPI /Лаб/	7	8	Экз, Кр
2	**Раздел 2. Самостоятельная работа**			
2.1	Контрольная работа /Тема/	7	0	
2.1.1	Выполнение контрольной работы по вариантам /Ср/	7	6	Экз, Кр
2.1.2	Проверка контрольной работы /Контр.раб./	7	35.65	Экз, Кр
3	**Раздел 3. Промежуточная аттестация**			
3.1	Экзамен /Тема/	7	0	
3.1.1	Экзамен /КоРа/	7	0.35	Экз, Кр

Примечание. Формы контроля: Эк – экзамен, К- контрольная работа, Ко- контрольный опрос, Сз- семестровое задание, З-зачет, ОП-отчет по практике.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства планируемых результатов обучения представлены в виде фондов оценочных средств (ФОС), разработанных в соответствии с локальным нормативным актом университета. ФОС может быть представлен в Приложении к рабочей программе.

5.1 Контрольные вопросы и задания

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.1: Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Результат обучения:знает основы крипторафической защиты информации.
Вопросы, задания:
1. Какие бывают виды шифрования?
2. Каковы основные базовые операции шифрования?
3. Сколько ключей применяется при симметричном шифровании?
4. Сколько ключей применяется при асимметричном шифровании?
5. Какие режимы шифрования блочных шифров бывают?

ОПК-3.2: Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности.

Результат обучения: умеет осуществлять настройку средств защиты информации (в то числе криптографической), применять знания защиты информации при реализации проектов в смежных областях.
Вопросы, задания:
1. Какие задачи решает применение удостоверяющих центров?
2. Каково назначение сертификата открытого ключа?
3. Сколько версий стандарта x509 существует?
4. Какие способы отзыва сертификата бывают?
5. Какие основные модели доверия УЦ применяются?

ОПК-3.3: Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.

Результат обучения: владеет навыками выбора средств защиты по требованиям к ним и их характеристиками, конфигурирования средств защиты в инфокоммуникационных системах.
Вопросы, задания:
1. Какие средства защиты информации строятся на базе криптографических алгоритмов?
2. Как применять интерфейс CryptoAPI при разработке приложений?
3. Какие базовые настройки необходимы для защиты электронной почты с использованием сертификатов открытых

ключей?
4. Как функционирует защита каналов связи по протоколу IPSec?
5. Как функционирует протокол Kerberos?

5.2 Темы письменных работ (контрольная работа)

На контрольную работу студенту выдается индивидуальное задание (по вариантам), заключающееся в разработке приложения с использованием методов защиты или в исследовании технологий информационной безопасности.

Работа оформляется в письменной форме в течение 10 недель с момента выдачи задания. Контрольный срок сдачи – последний месяц семестра.

Примерное содержание контрольной работы
1. Титульный лист.
2. Формулировка варианта задания.
3. Основная часть, включающая Описание алгоритма, метода решения, протокола безопасности.

Правила оформления контрольной работы
- контрольная работа оформляется в редакторе MS Word / OpenOffice (*.doc, *.docx, *.odt);
- листы формата А4, ориентация книжная;
- поля: левое – 2 см, остальные – по 1 см;
- шрифт – Times New Roman;
- размер шрифта 14 pt;
- междустрочный интервал – 1,5;
- абзацный отступ – 1,25 см;
- нумерация страниц сквозная, номер на первой странице не ставится;
- в конце работы необходим список использованной литературы согласно ГОСТ Р 7.0.5 – 2008;
- объем работы зависит от степени раскрытия основных пунктов контрольной работы.

Примерный список вариантов контрольной работы:

1. Организация защищенного web-соединения
2. Реализация системы инсталляции с лицензированием средствами Microsoft Visual Studio
3. Разработка программных средств защищенной аудио-видео трансляции
4. Реализация защиты от копирования экрана
5. Разработка программных средств контроля и блокирования устройств ввода-вывода ЭВМ

5.3 Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент может демонстрировать следующие уровни овладения компетенциями.

Повышенный уровень: обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий. Оценка промежуточной аттестации (зачет): 90 баллов и более.

Базовый уровень: обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий. Оценка промежуточной аттестации (зачет): 76-89 баллов.

Пороговый уровень: обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне. Оценка промежуточной аттестации (зачет): 61-75 баллов.

Уровень ниже порогового: система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности.
Оценка промежуточной аттестации (зачет): ниже 61 балла.

В рамках данной дисциплины используются следующие критерии оценки знаний студентов.

90 баллов и более
Обучающийся демонстрирует:
- систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы;
- точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы;
- безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;
- выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации;

- полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине;
- умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин;
- творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

76-89 баллов
Обучающийся демонстрирует:
- систематизированные, глубокие и полные знания по всем разделам учебной дисциплины;
- использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;
- владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач;
- способность решать сложные проблемы в рамках учебной дисциплины;
- свободное владение типовыми решениями;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине;
- умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку;
- активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

61-75 баллов
Обучающийся демонстрирует:
- достаточные знания в объеме рабочей программы по учебной дисциплине;
- использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать выводы без существенных ошибок;
- владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно применять типовые решения в рамках изучаемой дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой по дисциплине;
- умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине;
- работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

ниже 61 балла (не зачтено)
Обучающийся демонстрирует:
- фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине;
- неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок;
- пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

5.4. Вопросы промежуточной аттестации

1. Шифры замены. Одноалфавитные системы.
2. Шифр Цезаря. Шифр Цезаря с ключевым словом. Аффинная криптоси-стема. Шифр Полибия. Методы вскрытия одноалфавитных систем.
3. Многоалфавитные системы (шифр Вернама, шифр с автоключом).
4. Шифры перестановки (простой столбцевой перестановочный шифр, пе-рестановочный шифр с ключевым словом).
5. Схема Фейстеля. Режимы шифрования блочных шифров.
6. Алгоритм ГОСТ 28147-89. Основной шаг алгоритма.
7. Алгоритм ГОСТ 28147-89. Цикл алгоритма. Режим простой замены.
8. Алгоритм ГОСТ 28147-89. Режим гаммирования.
9. Алгоритм ГОСТ 28147-89. Режим гаммирования с обратной связью.
10. Алгоритм ГОСТ 28147-89. Режим выработки имитовставки.
11. DES, основной этап, описание принципа работы.
12. Потоковые шифры. Самосинхронизирующиеся потоковые шифры. Синхронные потоковые шифры.
13. Понятие хэш-функции. Передача информации с использованием криптографии с открытым ключом.
14. Инфраструктура открытых ключей (Общие понятия, необходимость ее создания)
15. Сертификат открытого ключа. Стандарт X.509
16. Механизмы проверки статуса сертификатов
17. Жизненный цикл ключа
18. Жизненный цикл сертификата.
19. CryptoAPI 1.0. CryptoAPI 2.0
20. Состав и назначение программных компонент Удостоверяющего Центра. Центр сертификации.
21. Состав и назначение программных компонент Удостоверяющего Центра. Центр регистрации.
22. Состав и назначение программных компонент Удостоверяющего Центра. АРМ абонента.
23. Модели доверия УЦ. Иерархическая модель.

24. Модели доверия УЦ. Сетевая модель.
25. Модели доверия УЦ. Мостовая модель.
26. Протокол TLS/SSL. Уровень диалога (рукопожатия).
27. Протокол TLS/SSL. Уровень записи.
28. Алгоритм работы Ipsec.

5.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности
Промежуточная аттестация обучающихся ведется непрерывно и включает в себя текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По данной дисциплине, завершающейся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов. Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (зачете).

Система оценивания

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести устный опрос, письменные задания, лабораторные работы, контрольные работы.

Контрольная работа
Контрольная работа по настоящей дисциплине представляет собой законченную работу, включающую в себя описание одного из современных вопросов системной инженерии.
Данная работа позволяет оценить умения учащихся решать практические. Полностью выполненная контрольная работа оценивается в 18 баллов.

Лабораторная работа.
Лабораторная работа является формой контроля и средством применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. За каждое полностью выполненное лабораторное задание начисляется 7 баллов. В рамках данной дисциплины планируется 6 лабораторных работ. Темы лабораторных работ указаны в разделе “4. Структура и содержание дисциплины (модуля, практики)”.

Устный опрос, собеседование.
Устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Устный ответ или собеседование может практиковаться преподавателем для уточнения знаний на практических и лабораторных занятиях.

Устный опрос включает 1 вопрос из группы вопросов “5.1 Контрольные вопросы и задания”, собеседование может включать более 1-го вопроса того же списка. Ответ оценивается от 0 до 3 баллов следующим образом:
3 балла - полный, логически безупречный ответ;
2 балла - ответ в целом полный, но могут иметь место несущественные пробелы в знаниях; логика ответа правильная, но некоторые моменты в своих рассуждениях студент обосновать затрудняется;
1 балл - ответ частичный, содержит значительные изъяны; нарушений логики ответа нет, но имеется ряд логических переходов в рассуждениях, которые студент обосновать затрудняется.

Промежуточная аттестация. Экзамен.
Промежуточная аттестация осуществляется в конце семестра и завершает изучение дисциплины. Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций. В рамках данного предмета к форме промежуточного контроля относится экзамен.

Экзамен по дисциплине имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Экзамен проводится в устной форме. В ходе зачета студент отвечает на вопросы билета. Билет включает два вопроса из списка "5.4. Вопросы промежуточной аттестации", оцениваемых по 20 баллов. Дополнительные баллы, помимо баллов, полученных за контрольные и письменную работы, могут быть заработаны за правильные ответы в ходе опросов и собеседований.

Если суммарное число баллов набранных в семестре по результатам модулей и полученных на экзамене
- от 61 до 100 , то ставится итоговая оценка "Зачтено",
- менее 61, то ставится итоговая оценка "Не зачтено".
Если суммарное число баллов, набранных студентом не менее 60 баллов, то студент может согласиться с соответствующей

итоговой оценкой без экзамена.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

6.1. Рекомендуемая литература

	Авторы, составители	Заглавие	Издательство, год.	Электронный адрес
Л.1	Олифер В. Г., Олифер Н. А.	Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для студ. вузов	СПб.: Питер, 2004	
Л.2	Лукьянов В. С., Черковский И. В., Скакунов А. В., Быков Д. В.	Модели компьютерных сетей с удостоверяющими центрами: монография	Волгоград: ВолгГТУ, 2009	
Л.3	Лукьянов В. С., Быков Д. В.	Методы обеспечения безопасности в сетях с публичными ключами: учеб. пособие	Волгоград: ВолгГТУ, 2015	
Л.4	Шевченко В. П.	Вычислительные системы, сети и телекоммуникации: учебник	Москва: КноРус, 2021	https://www.book.ru/book/936930
Л.5	Нестеров С. А.	Основы информационной безопасности: учеб. пособие	Санкт-Петербург: Лань, 2018	
Л.6	Бизяев А. А., Куратов К. А.	Сети связи и системы коммутации: учебное пособие	Новосибирск: НГТУ, 2016	https://e.lanbook.com/book/118257
Л.7	Эделман Дж., Лоу С. С., Осуолт М.	Автоматизация программируемых сетей	Москва: ДМК Пресс, 2019	https://e.lanbook.com/reader/book/123708/#2

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э2	Голиков, А. М. Тестирование и диагностика в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2016. — 436 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110274 (дата обращения: 19.09.2021). — Режим доступа: для авториз. пользователей.
Э3	Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э4	Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 376 с. — ISBN 978-5-8114-8515-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176658 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э5	Лукша, М. Kubernetes в действии / М. Лукша ; перевод с английского А. В. Логунов. — Москва : ДМК Пресс, 2019. — 672 с. — ISBN 978-5-97060-657-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131688 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э6	Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для вузов / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8051-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171410 (дата обращения: 18.09.2021). — Режим доступа: для авториз. пользователей.
Э7	Федеральный портал «Российское образование» [Электронный ресурс] – Режим доступа: www.edu.ru
Э8	Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс] – Режим доступа: www.intuit.ru
Э9	Защита информации в центрах обработки данных : учебно-методическое пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин, Т. Е. Захарова. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 44 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180094 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей.
Э10	Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148386 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей.

6.3 Перечень программного обеспечения

6.3.1.1	Операционная система Windows- Лекционные,практические занятия,самостоятельная работа обучающихся.
6.3.1.2	LibreOffice — офисный пакет - Лекционные,практические занятия,самостоятельная работа обучающихся.
6.3.1.3	VMWare - среда виртуализации
6.3.1.4	Visual Studio (или аналогичная среда разработки)

6.4 Перечень информационных справочных систем и электронных библиотечных систем (ЭБС)	
6.3.2.1	Библиотека (НТБ), http://library.vstu.ru/sci-nci
6.3.2.2	Электронная информационно-образовательная среда университета, http://eos2.vstu.ru
6.3.2.3	ЭБС "Лань", https://e.lanbook.com/
6.3.2.4	ЭБС "Book.ru", https://www.book.ru/
6.3.2.5	Электронная библиотека "Grebennikon", https://grebennikon.ru/
6.3.2.6	Библиографическая и реферативная база данных статей, опубликованных в научных изданиях “Scopus”,
6.3.2.7	https://www.scopus.com/
6.3.2.8	
6.3.2.9	Российская научная электронная библиотека, интегрированная с РИНЦ “eLIBRARY.ru”, https://www.elibrary.ru/
6.3.2.10	
6.3.2.11	Поисковая интернет-платформа, объединяющая реферативные базы данных публикаций в научных журналах и
6.3.2.12	патентов “Web of Science”, https://webofknowledge.com/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) /ОБОРУДОВАНИЕ	
7.1	1. Лаборатория сетевых технологий / Мультимедийный класс для проведения занятий лекционного и семинарского
7.2	типа, лабораторных занятий
7.3	1) ПЭВМ Intel DualCore 2ГГц / 2Гб RAM / LCD 19" - 8 шт.; 2) экран EliteScreens; 3) проектор Acer 1200; 4) Коммутаторы CISCO
7.4	2. Учебная лаборатория / комьютерный класс
7.5	1) Ноутбуки HP Elitebook 8460p – 4 шт., 2) Ноутбуки HP EliteBook 8570p - 4 шт. 3) Ноутбук Lenovo ThinkPad T420 – 4 шт. 4) экран EliteScreens; 5) проектор Acer 1203;
7.6	6) доступ в Интернет и к наукометрическим базам данных
7.7	3. Аудитория для самостоятельной работы обучающихся./Учебная мебель, компьютерная техника с возможностью
7.8	подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду
7.9	университета (читальный зал информационно-библиотечного центра)

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)

Организация образовательного процесса по данной дисциплине регламентируется учебным планом и расписанием учебных занятий. При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет дисциплины (переаттестации ее части), если она была освоена в процессе предшествующего обучения. Перезачёт (переаттестации ее части) освобождает обучающегося от необходимости повторного освоения дисциплины (полностью или частично).
Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и лабораторными работами. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в электронной информационной образовательной среде.
Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана. На первой лекции лектор информирует студентов о рекомендуемой литературе и электронных источниках информации по дисциплине, с указанием, какой учебник (учебное пособие) является базовым.
Лабораторные работы представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают основные разделы дисциплины. Основной формой проведения лабораторных работ является решение конкретных задач. Каждой лабораторной работе предшествует самостоятельная подготовка студента, включающая: ознакомление с содержанием лабораторной работы по методическим указаниям; проработку теоретической части по лекционному материалу и учебникам, рекомендованным в методических указаниях.
Самостоятельная работа студентов включает изучение законспектированного на лекционных занятиях материала, дополнение его с учетом рекомендованной по данной теме литературы, самостоятельную подготовку к лабораторным работам, самостоятельное выполнение и оформление заданий контрольной работы, аналогичных выполненным на занятиях.

Перечень методических указаний для освоения дисциплины:

1. Лукьянов, В. С. Методы обеспечения безопасности в сетях с публичными ключами [Электронный ресурс] : учеб. пособие / В. С. Лукьянов, Д. В. Бы-ков ; ВолгГТУ. - Волгоград : ВолгГТУ, 2015. - 80 с. - ISBN 978–5–9948–1916–6.

2. В. С. Лукьянов, С. С. Шевелев. Протоколы защиты информации в сетях. Уч. пособие. Волгоград: РПК «Политехник», 2002

В течении семестра для студентов проводятся групповые текущие консультации по учебной дисциплине.
Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов
Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ), индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.
В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн), в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.
Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ (при необходимости).
Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств. Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания.
При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.