



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образование
высшего образования
«Волгоградский государственный технический университет»



Факультет электроники и вычислительной техники

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

Безопасность корпоративных информационных
систем

рабочая программа дисциплины (модуля, практики)

Закреплена за кафедрой Электронно-вычислительные машины и системы
Учебный план Направление 09.04.01 Информатика и вычислительная техника
Программа "Анализ данных и интеллектуальные технологии"
Профиль
Квалификация Магистр
Срок обучения 2 года

Форма обучения очная
Виды контроля в семестрах: зачеты 4
Общая трудоемкость 4 ЗЕТ

Семестр(Курс.Номер семестра на курсе)	4(2.2)		Итого	
	УП	ПП	УП	ПП
Практические	12	12	12	12
Лабораторные	12	12	12	12
Итого ауд.	24	24	24	24
Контактная работа	24.25	24.25	24.25	24.25
Сам. работа	119.75	119.75	119.75	119.75
Часы на контроль	0	0	0	0
Практическая подготовка	0	0	0	0
Итого трудоемкость в часах	144	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)

Безопасность корпоративных информационных систем

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

составлена на основании учебного плана:

Направление 09.04.01 Информатика и вычислительная техника

Программа "Анализ данных и интеллектуальные технологии"

Профиль:

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

Рабочая программа дисциплины (модуля, практики) актуализирована 30.08.2024

СОГЛАСОВАНО:

Факультет электроники и вычислительной техники

Председатель НМС факультета: Авдеюк О.А.

Протокол заседания НМС от

г. №

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ). ВИД, ТИП ПРАКТИКИ, СПОСОБ И ФОРМА (ФОРМЫ) ЕЕ ПРОВЕДЕНИЯ.	
Формирование у студентов знаний и умений связанных с решением задач обеспечения безопасности корпоративных информационных систем	
Задачи:	
- изучение способов анализа угроз информационной безопасности КИС и основных общеметодологических принципов построения систем обеспечения информационной безопасности;	
- получение навыков использования основных методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, проведения аттестации защищаемых КИС.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДВ.04
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Программное обеспечение инфокоммуникационных систем
2.1.2	Современные операционные системы
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ, ПРАКТИКИ)	
ПК-4: Управление развитием инфокоммуникационной системы организации	
<i>ПК-4.1: Знает: основные направления развития инфокоммуникационной системы организации.</i>	
Результаты обучения: Знает основные направления развития инфокоммуникационной системы организации.	
<i>ПК-4.2: Умеет: управлять изменениями при обеспечении функционирования инфокоммуникационной системы организации.</i>	
Результаты обучения: Умеет управлять изменениями при обеспечении функционирования инфокоммуникационной системы организации.	
<i>ПК-4.3: Владеет навыками: применения современных инструментов поддержки инфокоммуникационной системы организации.</i>	
Результаты обучения: Владеет навыками применения современных инструментов поддержки инфокоммуникационной системы организации.	
ПК-5: Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения	
<i>ПК-5.1: Знает: основные принципы процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения.</i>	
Результаты обучения: Знает основные принципы процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения.	
<i>ПК-5.2: Умеет: выявлять и диагностировать ошибки сетевых устройств и программного обеспечения.</i>	
Результаты обучения: Умеет выявлять и диагностировать ошибки сетевых устройств и программного обеспечения.	
<i>ПК-5.3: Владеет навыками: применения современных инструментов поиска и диагностики ошибок сетевых устройств и программного обеспечения.</i>	
Результаты обучения: Владеет навыками применения современных инструментов поиска и диагностики ошибок сетевых устройств и программного обеспечения.	
ПК-11: Управление сервисами ИТ	
<i>ПК-11.1: Знает: основы управления сервисами ИТ.</i>	
Результаты обучения: Знает основы управления сервисами ИТ.	
<i>ПК-11.2: Умеет: управлять сервисами ИТ.</i>	
Результаты обучения: Умеет управлять сервисами ИТ.	
<i>ПК-11.3: Владеет навыками: применения современных инструментов управления сервисами ИТ.</i>	
Результаты обучения: Владеет навыками применения современных инструментов управления сервисами ИТ.	
ПК-13: Управление проектами в области ИТ малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта	
<i>ПК-13.1: Знает: технологии управления проектами в области ИТ.</i>	
Результаты обучения: Знает технологии управления проектами в области ИТ.	
<i>ПК-13.2: Умеет: применять методы управления проектами на практике.</i>	
Результаты обучения: Умеет применять методы управления проектами на практике.	

ПК-13.3: Владеет навыками: применения инструментов и программного обеспечения поддержки процесса управления проектами в ИТ малого и среднего уровня сложности в условиях неопределенности.

Результаты обучения: Владеет навыками применения инструментов и программного обеспечения поддержки процесса управления проектами в ИТ малого и среднего уровня сложности в условиях неопределенности.

ПК-17: Организация разработки системного программного обеспечения

ПК-17.1: Знает: основы организации разработки системного программного обеспечения.

Результаты обучения: Знает основы организации разработки системного программного обеспечения.

ПК-17.2: Умеет: организовывать и управлять процессом разработки системного программного обеспечения

Результаты обучения: Умеет организовывать и управлять процессом разработки системного программного обеспечения

ПК-17.3: Владеет навыками: использования современных средств организации и разработки системного программного обеспечения

Результаты обучения: Владеет навыками использования современных средств организации и разработки системного программного обеспечения

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	Методологические основы комплексной системы защиты информации КИС. Определение состава защищаемой информации /Тема/	4	0	
1.1.1	Определение состава защищаемой информации и нормативной базы для ее защиты /Пр/	4	2	3, Кр
1.1.2	Классификация КИС /Лаб/	4	2	3, Кр
1.2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации /Тема/	4	0	
1.2.1	Варианты осуществления НСД /Пр/	4	2	3, Кр
1.2.2	Защиты от НСД /Лаб/	4	2	3, Кр
1.3	Моделирование процессов комплексной системы защиты информации. Нормативно-методическое обеспечение систем защиты информации. Управление комплексной системой защиты информации /Тема/	4	0	
1.3.1	Порядок составления МУН /Пр/	4	2	3, Кр
1.3.2	Разработка МУН для тестовой системы /Лаб/	4	2	3, Кр
1.4	Предпроектное обследование. Аналитическое обоснование необходимости создания СЗИ /Тема/	4	0	
1.4.1	Порядок проведения предпроектного обследования /Пр/	4	2	3, Кр
1.4.2	Оформления отчета об обследовании /Лаб/	4	2	3, Кр
1.5	Техническое (частное техническое) задание на разработку СЗИ. Проектирование комплексной системы защиты информации /Тема/	4	0	
1.5.1	Структура ТЗ на систему защиты /Пр/	4	2	3, Кр
1.5.2	Разработка ТЗ на систему защиты /Лаб/	4	2	3, Кр
1.6	Технический проект КСЗИ. Политика информационной безопасности /Тема/	4	0	
1.6.1	Структура ТП /Пр/	4	2	3, Кр
1.6.2	Разработка ТП на систему защиты /Лаб/	4	2	3, Кр
2	Раздел 2. Самостоятельная работа студентов			
2.1	Подготовка к отчету лабораторных работ и практическим занятиям /Тема/	4	0	
2.1.1	Подготовка к отчетам /Ср/	4	40	3, Кр
2.2	Выполнение контрольной работы /Тема/	4	0	
2.2.1	Выполнение Контрольной работы /Ср/	4	79.75	3, Кр
3	Раздел 3. Промежуточная аттестация			
3.1	Зачет /Тема/	4	0	
3.1.1	Зачет /КоПа/	4	0.25	3, Кр

Примечание. Формы контроля: Эк – экзамен, К- контрольная работа, Ко- контрольный опрос, Сз- семестровое задание, 3-зачет, ОП- отчет по практике, Зд-задание, Р-реферат.

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

Приложения к рабочей программе.

5.1 Контрольные вопросы и задания

ПК-4: Управление развитием инфокоммуникационной системы организации

ПК-4.1: Знает: основные направления развития инфокоммуникационной системы организации.

Студент должен знать основные направления развития инфокоммуникационной системы организации.

ПК-4.2: Умеет: управлять изменениями при обеспечении функционирования инфокоммуникационной системы организации.

Студент должен уметь управлять изменениями при обеспечении функционирования инфокоммуникационной системы организации.

ПК-4.3: Владеет навыками: применения современных инструментов поддержки инфокоммуникационной системы организации.

Студент должен владеть навыками применения современных инструментов поддержки инфокоммуникационной системы организации.

Вопросы, задания:

1. Какие основные принципы обеспечения ИБ?
2. На какие направления можно декомпозировать задачу обеспечения ИБ?
3. Каковы основные участники процесса обеспечения ИБ при разработке программного и аппаратного обеспечения ИС?
4. Каковы основные стадии процесса обеспечения ИБ при разработке программного и аппаратного обеспечения ИС?
5. Какие группы нормативной документации применяются при обеспечении ИБ?

ПК-5: Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения

ПК-5.1: Знает: основные принципы процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения.

Студент должен знать основные принципы процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения.

ПК-5.2: Умеет: выявлять и диагностировать ошибки сетевых устройств и программного обеспечения.

Студент должен уметь выявлять и диагностировать ошибки сетевых устройств и программного обеспечения.

ПК-5.3: Владеет навыками: применения современных инструментов поиска и диагностики ошибок сетевых устройств и программного обеспечения.

Студент должен владеть навыками применения современных инструментов поиска и диагностики ошибок сетевых устройств и программного обеспечения.

Вопросы, задания:

1. Опишите построения системы защиты в рамках разработки программного и аппаратного обеспечения КИС
2. Приведите примеры документов, которые формируются при построении системы защиты в рамках разработки программного и аппаратного обеспечения КИС
3. Какие классы СЗИ применяются при проектировании системы защиты в рамках разработки программного и аппаратного обеспечения КИС?
4. Опишите организационные мероприятия, которые должны применяться при внедрении системы защиты в рамках разработки программного и аппаратного обеспечения КИС
5. Опишите виды и методы испытаний, которые должны проводиться после внедрения системы защиты в рамках разработки программного и аппаратного обеспечения КИС

ПК-11: Управление сервисами ИТ

ПК-11.1: Знает: основы управления сервисами ИТ.

Студент должен знать основы управления сервисами ИТ.

ПК-11.2: Умеет: управлять сервисами ИТ.

Студент должен уметь управлять сервисами ИТ.

ПК-11.3: Владеет навыками: применения современных инструментов управления сервисами ИТ.

Студент должен владеть навыками применения современных инструментов управления сервисами ИТ.

Вопросы, задания:

1. Каков порядок построения системы защиты в рамках модернизации программного и аппаратного обеспечения КИС?
2. Какие основные документы разрабатываются при построении системы защиты?
3. Какие классы СЗИ применяются при проектировании системы защиты в рамках модернизации программного и аппаратного обеспечения КИС?
4. Каковы организационные мероприятия, которые должны применяться при внедрении системы защиты?
5. Какие виды и методы испытаний должны проводиться после внедрения системы защиты?

ПК-13: Управление проектами в области ИТ малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта

ПК-13.1: Знает: технологии управления проектами в области ИТ.

Студент должен знать технологии управления проектами в области ИТ.

ПК-13.2: Умеет: применять методы управления проектами на практике.

Студент должен уметь применять методы управления проектами на практике.

ПК-13.3: Владеет навыками: применения инструментов и программного обеспечения поддержки процесса управления проектами в ИТ малого и среднего уровня сложности в условиях неопределенности.

Студент должен владеть навыками применения инструментов и программного обеспечения поддержки процесса управления проектами в ИТ малого и среднего уровня сложности в условиях неопределенности.

Вопросы, задания:

1. Приведите примеры требований, которые должны учитываться при выборе средств защиты
2. Опишите, какие задачи решают и какими возможностями обладают средства защиты информации от несанкционированного доступа
3. Опишите, какие задачи решают и какими возможностями обладают сетевые средства защиты информации
4. Опишите, какие задачи решают и какими возможностями обладают криптографические средства защиты информации
5. Опишите, какие задачи решают и какими возможностями обладают средства антивирусной защиты и анализа защищенности

ПК-17: Организация разработки системного программного обеспечения

ПК-17.1: Знает: основы организации разработки системного программного обеспечения.

Студент должен знать основы организации разработки системного программного обеспечения.

ПК-17.2: Умеет: организовывать и управлять процессом разработки системного программного обеспечения

Студент должен уметь организовывать и управлять процессом разработки системного программного обеспечения

ПК-17.3: Владеет навыками: использования современных средств организации и разработки системного программного обеспечения

Студент должен владеть навыками использования современных средств организации и разработки системного программного обеспечения

5.2 Темы письменных работ (контрольная работа)

На контрольную работу студенту выдается индивидуальное задание (по вариантам), заключающееся в разработке документа «Модель угроз и нарушителя безопасности».

Работа выполняется 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:
 - 1) Описание объекта защиты, для которого производится моделирование угроз.
 - 2) Определение негативных последствий от реализации (возникновения) угроз безопасности информации.
 - 3) Определение возможных объектов воздействия угроз безопасности информации.
 - 4) Определение источников угроз безопасности информации.
 - 5) Оценка способов реализации (возникновения) угроз безопасности информации.
 - 6) Оценка актуальности угроз безопасности информации.

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. Разработка модели угроз и нарушителя для типовой КИС
2. Разработка технического задания на систему защиты для типовой КИС
3. Разработка ответа о предпроектном обследовании для типовой КИС

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, не зачтено.

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.

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. Какие основные принципы обеспечения ИБ при разработке программного и аппаратного обеспечения ИС?

2. На какие направления можно декомпозировать задачу обеспечения ИБ при разработке программного и аппаратного обеспечения ИС?

3. Каковы основные участники процесса обеспечения ИБ при разработке программного и аппаратного обеспечения ИС?

4. Каковы основные стадии процесса обеспечения ИБ при разработке программного и аппаратного обеспечения ИС?
5. Какие группы нормативной документации применяются при обеспечении ИБ при разработке программного и аппаратного обеспечения ИС?
6. Каков порядок анализа угроз ИБ по методике ФСТЭК России?
7. Какова структура карточек в Банке данных угроз ФСТЭК России?
8. Какова связь между уязвимостью и угрозой ИБ?
9. Как связаны техники и тактики, согласно методике моделирования угроз ФСТЭК России?
10. Какие основные категории нарушителей применяются при анализе угроз ИБ?
11. Какие основные принципы обеспечения ИБ при модернизации программного и аппаратного обеспечения ИС?
12. На какие направления можно декомпозировать задачу обеспечения ИБ при модернизации программного и аппаратного обеспечения ИС?
13. Каковы основные участники процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения ИС?
14. Каковы основные стадии процесса обеспечения ИБ при модернизации программного и аппаратного обеспечения ИС?
15. Какие группы нормативной документации применяются при обеспечении ИБ при модернизации программного и аппаратного обеспечения ИС?
16. Какова структура документа «Модели угроз и нарушителя безопасности»?
17. Как определяются актуальные нарушители ИБ?
18. Как определяются актуальные угрозы ИБ?
19. Как результаты моделирования угроз влияют на требования по обеспечению ИБ?
20. Каковы основные подходы по выбору средств защиты для нивелирования актуальных угроз ИБ?

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) и семестровую аттестацию (зачет) – оценивание окончательных результатов обучения по дисциплине.

По данной дисциплине, завершающейся зачетом, 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 представляет собой законченную работу, включающую в себя разработку документа «Модель угроз и нарушителя безопасности». Данная работа позволяет оценить умения учащихся решать практические задачи моделирования угроз, умения ориентироваться в информационном пространстве по данной тематике, оценить уровень сформированности аналитических навыков. Полностью выполненная контрольная работа оценивается в 30 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. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. За каждое полностью выполненное лабораторное задание начисляется 10 баллов. В рамках данной дисциплины планируется 3 лабораторные работы. 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 обучающимися 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. Зачет.

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 зачет.

Зачет 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. Зачет проводится в устной форме. В ходе зачета студент готовит ответы на вопросы билета. Билет включает два вопроса из списка "5.4. Вопросы промежуточной аттестации", оцениваемых по 20 баллов. Дополнительные баллы, помимо баллов, полученных за контрольную и лабораторные 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 зачете

- от 61 до 100, то ставится итоговая оценка "Зачтено",

- менее 61 балла, то ставится оценка "Не зачтено".

Если суммарное число баллов, набранных студентом не менее 60 баллов, то студент может согласиться с соответствующей итоговой оценкой без зачета.

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

6.1. Рекомендуемая литература

	Авторы, составители	Заглавие	Издательство, год.	Электронный адрес
Л1.1	Олифер В. Г., Олифер Н. А.	Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для студ. вузов	СПб.: Питер, 2004	
Л1.2	Лукьянов В. С., Быков Д. В.	Методы обеспечения безопасности в сетях с публичными ключами: учеб. пособие	Волгоград: ВолгГТУ, 2015	
Л1.3	Шевченко В. П.	Вычислительные системы, сети и телекоммуникации: учебник	Москва: КноРус, 2021	https://www.book.ru/book/936930
Л1.4	Нестеров С. А.	Основы информационной безопасности: учеб. пособие	Санкт-Петербург: Лань, 2018	
Л1.5	Бизяев А. А., Куратов К. А.	Сети связи и системы коммутации: учебное пособие	Новосибирск: НГТУ, 2016	https://e.lanbook.com/book/118257
	Авторы, составители	Заглавие	Издательство, год.	Электронный адрес
Л2.1	Лукьянов В. С., Черковский И. В., Скакунов А. В., Быков Д. В.	Модели компьютерных сетей с удостоверяющими центрами: монография	Волгоград: ВолгГТУ, 2009	
Л2.2	Ли П., Райтман М. А.	Архитектура интернета вещей	Москва: ДМК Пресс, 2019	https://e.lanbook.com/reader/book/112923/#5

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 : ГУСОР, 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	OpenOffice, LibreOffice – офисные пакеты
6.3.1.2	Microsoft Visual Studio Community – среда разработки
6.3.1.3	Яндекс.Браузер - веб-браузер.

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 / компьютерный 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 практическими занятиями. 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.

Практические занятия проводятся в целях рассмотрения основных вопросов курса и охватывают основные разделы дисциплины.

Основной формой проведения практических занятий является решение конкретных задач, аналогичные которым будут выполнять студенты на лабораторных работах.

Лабораторные работы предполагают выполнение и отчет заданий по темам, рассмотренным на практических занятиях. Каждому лабораторному занятию предшествует самостоятельная подготовка студента, включающая: ознакомление с содержанием лабораторной работы по методическим указаниям; проработку теоретической части по учебникам, рекомендованным в методических указаниях;

Самостоятельная работа студентов включает изучение законспектированного 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.

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 needs 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.