Подписано цифровой подписью: ОЧУ ВО "ЕВРЕЙСКИЙ УНИВЕРСИТЕТ"
Дата: 2023.11.14 14:05:26 +03'00'

ЕВРЕЙСКИЙ УНИВЕРСИТЕТ
ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

+7 495 736 9270
127273, г. Москва, ул. Отрадная, д.6
www.j-univer.ru

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Направление подготовки:
38.04.01 Экономика

Направленность (профиль)
Цифровой маркетинг

Уровень высшего образования: магистратура

Москва – 2023

1. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность в современном информационном пространстве» включена в часть, формируемую участниками образовательных отношений Блока I.

2. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РАМКАХ ИЗУЧАЕМОЙ ДИСЦИПЛИНЫ

Код компетенции	Формулировка компетенций в соответствии с ФГОС ВО
ПК-3	Способен разрабатывать, внедрять и совершенствовать систему маркетинговых коммуникаций в организации

2.1. Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями образовательной программы

Коды и формулировка компетенции	Индикаторы достижения компетенции	Запланированные результаты обучения
ПК-3 Способен разрабатывать, внедрять и совершенствовать систему маркетинговых коммуникаций в организации	ПК-3.1 – определяет конкурентоспособность ассортимента товаров и услуг организации с обоснованием их внедрения на рынок ПК-3.2 – проводит тестирование товаров (услуг) при внедрении их на рынок ПК-3.3 – создает нематериальные активы организации ПК-3.4 – управляет бизнес-процессами организации в сфере маркетинга, в т.ч. цифрового	**Знать:** типы информационных угроз информационному пространству; способы защиты от киберугроз при реализации маркетинговых программ; методы формирования маркетинговых программ. **Уметь:** осуществлять учет киберугроз при формировании целей маркетинговых программ; оптимизировать затраты на защиту маркетинговой деятельности компании в сети Интернет; применять методы защиты информационных ресурсов компании при осуществлении маркетинговой деятельности **Владеть:** навыками оценки уровня угроз при реализации маркетинговой программы, соотносить составляющие маркетинговых программ и элементы комплекса маркетинга; оптимизировать ресурсы при выборе инструментов защиты от киберпреступлений при реализации маркетинговых программ

3. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Структура учебной дисциплины для обучающихся очно-заочной формы обучения

Структура и объем дисциплины		Объем дисциплины по семестрам по очной ф.о.	Объем дисциплины по семестрам по очно-заочной ф.о.
Объем дисциплины в зачетных единицах			4
Объем дисциплины в часах			144
Аудиторные занятия (всего)			54
в том числе в часах:	Лекции (Л)		18
	Практические занятия (ПЗ)		36
	Лабораторные работы (ЛР)		
	Индивидуальные занятия (ИЗ)		
Самостоятельная работа студента в семестре, час			90
Самостоятельная работа студента в период промежуточной аттестации, час			
Форма промежуточной аттестации			
Зачет (зач.)			зачет
Дифференцированный зачет (диф.зач.)			
Экзамен (экз.)			

4. СОДЕРЖАНИЕ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Разделы дисциплины и виды учебной работы

№ п/п	Разделы дисциплины и виды занятий	Трудоёмкость в часах					Форма текущего и итогового контроля
		Лекции	Практические занятия	Самостоятельная работа студентов	Контроль	Зачетных единиц	
1	Лекция 1. Основные понятия в области защиты информации. Практическое занятие 1.	2	4	10			Устный опрос; индивидуальное задание
2	Лекция 2. Угрозы безопасности информационной системе. Практическое занятие 2.	2	4	10			Устный опрос; индивидуальное задание
3	Лекция 3. Организационные и физические меры защиты информации. Практическое занятие 3.	2	4	10			Устный опрос; индивидуальное задание
4	Лекция 4. Биометрические средства защиты информации. Практическое занятие 4.	2	4	12			Устный опрос; индивидуальное задание
5	Лекция 5. Кодирование и перекодирование информации. Практическое занятие 5.	2	4	12			Устный опрос; индивидуальное задание
6	Лекция 6. Пароли. Практическое занятие 6.	2	4	12			Устный опрос; индивидуальное задание
7	Лекция 7. Защита исполняемых программ. Практическое занятие 7.	2	4	12			Устный опрос; индивидуальное задание
8	Лекция 8. Защита носителей информации. Практическое занятие 8.	4	8	12			Устный опрос; индивидуальное задание
	Итого	18	36	90	-		Зачет

4.2. Лекционное занятие

№ п/п	Тема лекции	Трудоёмкость, час.	Образовательные технологии
1	Доктрина информационной безопасности Российской Федерации; Федеральный закон «Об информации, информационных технологиях и защите информации».	2	Презентация
2	Классификация уязвимостей информационной системы; Классификация угроз потери информации.	2	Презентация
3	Организационные меры по защите информации; Задачи, решаемые с помощью организационных мер.	2	Презентация
4	Качество биометрической системы ограничения доступа; Биологические параметры, используемые в системах ограничения доступа; Идентификационные задачи, решаемые	2	Презентация

№ п/п	Тема лекции	Трудоёмкость, час.	Образовательные технологии
	аппаратурой биометрического контроля доступа		
5	Кодирование информации, вводимой в компьютер; Понятие кодовой таблицы (страницы); Тип (формат или расширение имени файла) как признак определённой кодировки.	2	Презентация
6	Понятие и назначение пароля; объекты, доступ к которым ограничивают пароли; Современные требования к составлению паролей; Классификация паролей.	2	Презентация
7	«Воздействия», от которых следует защищать программы; Юридические виды распространения программ (Лицензионные и иные виды программ); Механизмы защиты программ.	2	Презентация
8	Защита структур (файлов и папок), сохраняемых на носителях; Контейнерная защита.	4	Презентация
	Итого	18	

4.3. Практическое занятие

№ п/п	Тема практического занятия	Трудоёмкость, час.	Образовательные технологии
1	Государственный стандарт РФ «Делопроизводство и архивное дело. Термины и определения»; Распределение ответственности за реализацию мер по защите информации. Федеральный закон «Об электронной подписи» Федеральный закон «О персональных данных». Цели защиты информации.	4	Устный опрос; индивидуальное задание
2	Возможные каналы утечки информации; Уголовная ответственность за преступления в сфере компьютерной информации.	4	Устный опрос; индивидуальное задание
3	Физические меры по защите информации; Макрофункции физической защиты и их состав.	4	Устный опрос; индивидуальное задание
4	Пластиковые карты как средство разрешения доступа или получения полномочий. Виды и особенности различных пластиковых карт. Особенности авторизации пластиковых карт, PIN код.	4	Устный опрос; индивидуальное задание
5	Перекодирование стандартными и офисными программами; Перекодирование и создание собственной кодировки специальными программами.	4	Устный опрос; индивидуальное задание
6	Виды атак на пароли; Способы запоминания надежных паролей.	4	Устный опрос; индивидуальное задание
7	Шифрование и упаковка программ; Полезные советы по защите программ.	4	Устный опрос; индивидуальное задание
8	Защита CD-ROM, DVD, BluRay; Региональная	8	Устный опрос;

№ п/п	Тема практического занятия	Трудоёмкость, час.	Образовательные технологии
	защита носителей.		индивидуальное задание
	Итого	36	

4.4. Самостоятельная работа студентов

№ п/п	Виды учебных занятий	Содержание самостоятельной работы	Трудоёмкость, час.	Форма текущего и итогового контроля
1	Лекция 1. Практическое занятие 1	Самостоятельное изучение материала темы 1; чтение дополнительной литературы; подготовка к устному опросу	10	Участие в устном опросе
2	Лекция 2. Практическое занятие 2	Самостоятельное изучение материала темы 2; чтение дополнительной литературы; подготовка к устному опросу; выполнение индивидуального задания	10	Устный опрос; индивидуальное задание
3	Лекция 3. Практическое занятие 3	Самостоятельное изучение материала темы 3; чтение дополнительной литературы; подготовка к устному опросу; выполнение индивидуального задания	10	Устный опрос; индивидуальное задание
4	Лекция 4. Практическое занятие 4	Самостоятельное изучение материала темы 4; чтение дополнительной литературы; подготовка к устному опросу; выполнение индивидуального задания	12	Устный опрос; индивидуальное задание
5	Лекция 5. Практическое занятие 5	Самостоятельное изучение материала темы 5; чтение дополнительной литературы; подготовка к устному опросу; выполнение индивидуального задания	12	Устный опрос; индивидуальное задание
6	Лекция 6. Практическое занятие 6	Самостоятельное изучение материала темы 6; чтение дополнительной литературы; подготовка к устному опросу; выполнение индивидуального задания	12	Устный опрос; индивидуальное задание
7	Лекция 7. Практическое занятие 7	Самостоятельное изучение материала темы 7; чтение дополнительной литературы; подготовка к устному опросу; выполнение индивидуального задания	12	Устный опрос; индивидуальное задание
8	Лекция 8. Практическое занятие 8	Самостоятельное изучение материала темы 8; чтение дополнительной литературы;	12	Устный опрос; индивидуальное задание

№ п/п	Виды учебных занятий	Содержание самостоятельной работы	Трудоёмкость, час.	Форма текущего и итогового контроля
		подготовка к устному опросу; выполнение индивидуального задания		
	Итого		90	

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

5.1 Связь результатов освоения дисциплины с уровнем сформированности заявленных компетенций в рамках изучаемой дисциплины

Код и наименование универсальной компетенции	Код и наименование индикатора достижения компетенции
ПК-3. Способен разрабатывать, внедрять и совершенствовать систему маркетинговых коммуникаций в организации	ПК-3.1 – определяет конкурентоспособность ассортимента товаров и услуг организации с обоснованием их внедрения на рынок ПК-3.2 – проводит тестирование товаров (услуг) при внедрении их на рынок ПК-3.3 – создает нематериальные активы организации ПК-3.4 – управляет бизнес-процессами организации в сфере маркетинга, в т.ч. цифрового

5.2 Оценочные средства для студентов с ограниченными возможностями здоровья

Оценочные средства для лиц с ограниченными возможностями здоровья выбираются с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Категории студентов	Виды оценочных средств	Форма контроля	Шкала оценивания
С нарушением слуха	Тесты, рефераты, контрольные вопросы	Преимущественно письменная проверка	В соответствии со шкалой оценивания, указанной в Таблице 5
С нарушением зрения	Контрольные вопросы	Преимущественно устная проверка (индивидуально)	
С нарушением опорно-двигательного аппарата	Решение тестов, контрольные вопросы дистанционно.	Письменная проверка, организация контроля с использование информационно-коммуникационных технологий.	

6. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ И ДРУГИЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ ЗАЯВЛЕННЫХ КОМПЕТЕНЦИЙ В РАМКАХ ИЗУЧАЕМОЙ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Семестр № 2

6.1. Вопросы для устного опроса

1. Компьютерная информация: определение, основные категории с точки зрения безопасности.
2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности.
3. Критерии надежности систем, классы безопасности.
4. Правовые основы защиты информации в РФ.
5. Обзор законов РФ в области информационной безопасности.
6. Дискреционная и мандатная модель доступа к объектам информационных систем.
7. Классификация угроз информационным системам.
8. Фундаментальные, базовые и первичные угрозы.
9. Троянская программа: назначение, классификация, руткиты как средство маскировки.
10. Методики защиты от вредоносных программ.
11. Модель безопасности ОС Windows.

12. Реализация дискреционной модели защиты доступа к ресурсам системы.
13. Аудит событий безопасности современных операционных систем.
14. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.

6.2. Примеры индивидуальных заданий

1. Исследование методов защиты программ от несанкционированного запуска. Исследовать методики, разрешающие запускать программу только на конкретной программно-аппаратной платформе и запрещающие ее запуск на других компьютерах. Рассмотреть несколько вариантов реализации подобной защиты, способы обхода такой защиты. Программно реализовать один из рассмотренных методов.
2. Исследование методов защиты программ от отладчиков. Рассмотреть методы, защищающие исследование кода отладчиками, проанализировать их стойкость к обходу защиты. Программно реализовать один из методов защиты, предотвращающий запуск программы из-под отладчика или затрудняющий анализ ее выполнения под отладчиком.
3. Исследование методов стеганографии (контейнер – графический файл). Рассмотреть методы стеганографического встраивания информации в графические контейнеры различных типов, проанализировать возможные атаки на стегоконтейнеры. Программно реализовать стеганографическое встраивание текстовой строки в графический контейнер и выделение ранее встроенной строки из стегоконтейнера. Проанализировать максимальное допустимое соотношение длины встраиваемой строки и размера графического контейнера, обеспечивающее секретность встраивания.
4. Исследование методов стеганографии (контейнер – аудио-файл). Рассмотреть методы стеганографического встраивания информации в аудио-контейнеры различных типов, проанализировать возможные атаки на стегоконтейнеры. Программно реализовать стеганографическое встраивание текстовой строки в аудиоконтейнер и извлечение ранее встроенной строки из стегоконтейнера. Проанализировать максимальное допустимое соотношение длины встраиваемой строки и размера контейнера, обеспечивающее секретность встраивания.
5. Разработка системы сертификации открытых ключей. Программная система должна генерировать ключевую пару открытый-закрытый ключ и генерировать сертификат для открытого ключа, подписанный корневым ключом системы. Реализовать возможность проверки подлинности открытого ключа по его сертификату.
6. Исследование программных интерфейсов управления доступом к ресурсам операционной системы. Рассмотреть различные программные интерфейсы для управления правами доступа пользователей и групп пользователей к ресурсам операционной системы (файлам, папкам, процессам и пр.). Программно реализовать возможность изменения прав доступа произвольной учетной записи или группы к ресурсам операционной системы.
7. Исследование атаки типа «переполнение буфера» и методов борьбы с ними. Рассмотреть различные варианты реализации атаки типа «переполнение буфера», проиллюстрировать рассмотренные варианты программным кодом. Модифицировать атакуемый код таким образом, чтобы атаки стали неэффективными.
8. Исследование принципов работы клавиатурных шпионов и методов борьбы с ними. Рассмотреть методики реализации клавиатурных шпионов, программно реализовать один из них. Описать основные способы предотвращения атак подобного типа.
9. Реализация системы аутентификации на основе клавиатурного почерка. Исследовать методы аутентификации пользователя на основе его клавиатурного почерка – особенностей ввода информации с клавиатуры. Реализовать подсистему аутентификации пользователя, основанную на анализе его клавиатурного почерка. При регистрации пользователя ему предлагается несколько раз ввести строку текста. Усредненные параметры ввода принимается за эталон пользовательского почерка. При входе пользователя в систему ему предлагается ввести ту же строку, что и при регистрации. При

совпадении параметров ввода с сохраненными для данного пользователя ему предоставляется доступ к программе, иначе фиксируется неудачная аутентификация.

10. Реализация системы распределенной аутентификации типа «запрос-ответ». Реализовать систему удаленной парольной аутентификации пользователя по схеме ”запрос-ответ”. Клиент и сервер должны обмениваться по сети аутентификационными пакетами для предотвращения атак типа перехват пароля, повторное воспроизведение, компрометация проверяющего.
11. Исследование методов генерации криптостойких случайных чисел с проверкой по тестам FIPS-140. Исследовать методы генерации случайных чисел, удовлетворяющих тестам криптостойкости FIPS-140. Программно реализовать генератор случайных чисел по одному из рассмотренных алгоритмов, осуществить проверку генерируемых чисел по стандарту FIPS-140.
12. Атаки типа «SQL-инъекция» и методы борьбы с ними. Исследовать уязвимости SQL-запросов, практически проиллюстрировать их на тестовой базе данных. Рассмотреть основные методы защиты от SQL-инъекции и продемонстрировать неэффективность ранее рассмотренных атак для модифицированных (защищенных) запросов к базам данных.
13. Исследование методов стеганографии (контейнер – текст). Рассмотреть методы стеганографического встраивания информации в текстовый контейнер, проанализировать возможные атаки на стегоконтейнер. Программно реализовать стеганографическое встраивание текстовой строки в контейнер-текстовый файл и извлечение ранее встроенной строки из стегоконтейнера. Проанализировать максимальное допустимое соотношение длины встраиваемой строки и размера контейнера, обеспечивающее секретность встраивания.
14. Исследование методов генерации сверхбольших простых чисел с проверкой на простоту. Рассмотреть методы генерации сверхбольших (до 1024 бит) простых чисел, а также алгоритмы вероятностной проверки чисел на простоту (Рабин-Миллер, Соловей-Штрассер, Леман…). Реализовать один из рассмотренных методов в виде программной системы, генерирующих простые числа заданной длины с заданной вероятностью их простоты.

6.3. Оценочные средства итогового контроля

Вопросы к зачету

1. Доктрина информационной безопасности Российской Федерации.
2. Федеральный закон «Об информации, информационных технологиях и защите информации».
3. Классификация уязвимостей информационной системы.
4. Классификация угроз потери информации.
5. Организационные меры по защите информации.
6. Задачи, решаемые с помощью организационных мер.
7. Качество биометрической системы ограничения доступа.
8. Биологические параметры, используемые в системах ограничения доступа.
9. Идентификационные задачи, решаемые аппаратурой биометрического контроля доступа.
10. Кодирование информации, вводимой в компьютер.
11. Понятие кодовой таблицы (страницы).
12. Тип (формат или расширение имени файла) как признак определённой кодировки.
13. Понятие и назначение пароля; объекты, доступ к которым ограничивают пароли.
14. Современные требования к составлению паролей; Классификация паролей.
15. «Воздействия», от которых следует защищать программы.
16. Юридические виды распространения программ (Лицензионные и иные виды программ).
17. Механизмы защиты программ.
18. Защита структур (файлов и папок), сохраняемых на носителях; Контейнерная защита.

19. Государственный стандарт РФ «Делопроизводство и архивное дело. Термины и определения».
20. Распределение ответственности за реализацию мер по защите информации.
21. Федеральный закон «Об электронной подписи».
22. Федеральный закон «О персональных данных».
23. Цели защиты информации.
24. Возможные каналы утечки информации.
25. Уголовная ответственность за преступления в сфере компьютерной информации.
26. Физические меры по защите информации.
27. Макрофункции физической защиты и их состав.
28. Пластиковые карты как средство разрешения доступа или получения полномочий.
29. Виды и особенности различных пластиковых карт.
30. Особенности авторизации пластиковых карт, PIN код.
31. Перекодирование стандартными и офисными программами.
32. Перекодирование и создание собственной кодировки специальными программами.
33. Виды атак на пароли.
34. Способы запоминания надежных паролей.
35. Шифрование и упаковка программ.
36. Полезные советы по защите программ.
37. Защита CD-ROM, DVD, BluRay.
38. Региональная защита носителей.

7.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

№	Наименование учебных аудиторий (лабораторий) и помещений для самостоятельной работы	Перечень оборудования и технических средств обучения	Программное обеспечение, в т.ч. отечественного производства
1	Учебные аудитории для проведения занятий лекционного типа	Преподавательский стол; столы обучающихся; стулья; классная доска; мультимедийный комплекс; наглядные пособия (плакаты) *Место, оборудованное для лиц с ограниченными возможностями.* Лицензионное программное обеспечение, подключенное к сети Интернет	7-Zip (Бесплатное ПО); 10-Strike Network Inventory ПО РФ (ПО) Duductor Academic ПО РФ (Бесплатное ПО); https://basegroup.ru/deductor/manual/licence-deductor-academic Eset Endpoint security (Платное ПО) https://help.eset.com/eula/ GIMP (Бесплатное ПО); https://docs.gimp.org/2.10/ru/ microsoft office проффесиональный плюс 2016 (ПО) https://www.microsoft.com/en-us/Useterms/Retail/Office/2016Professional/Useterms_Retail_Office_2016Professional_RUS.htm Microsoft power Bi (Бесплатное ПО); https://powerbi.microsoft.com/ru-ru/windows-license-terms/ icrosoft Visual Studio (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mt171584/ Notepad ++ (Бесплатное ПО); https://www.gnu.org/licenses/old-licenses/gpl-2.0.html Zoom (Бесплатное ПО); https://explore.zoom.us/ru/terms/ Anaconda3 2019 (Бесплатное ПО); https://www.anaconda.com/eula-anaconda-individual-edition Android studio (Бесплатное ПО); https://developer.android.com/studio/terms Brackets (Бесплатное ПО); https://github.com/brackets-cont/brackets/blob/master/LICENSE CodeBlocks (Бесплатное ПО);https://www.codeblocks.org/license/ Firebird (Бесплатное ПО); https://firebirdsql.org/en/licensing/ KNIME analytics platform (Бесплатное ПО); https://www.knime.com/downloads/full-license Loginom community РФ ПО (Бесплатное ПО);https://loginom.ru/legal Monogame SDK (Бесплатное ПО); https://github.com/MonoGame/MonoGame/blob/develop/LICENSE.txt Openproj (Бесплатное ПО); https://opensource.org/licenses/CPAL-1.0 tableau 2019 (Бесплатное ПО); https://www.tableau.com/legal Visual studio community 2017 (Бесплатное ПО);

			https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-qZeRxv7zAhXhsYsKHZoRBAsQFnoECBgQAQ&url=https%3A%2F%2Fvisualstudio.microsoft.com%2Fwp-con-tent%2Fuploads%2F2017%2F01%2FVS2017_COMMUNITY_RC_RUS_Eula.1049-1.docx&usg=AOvVaw0tLxlQA4E2McNypfRn9tTo Visual studio community 2019 (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mlt110718/ Консультант плюс
2	Компьютер-ный класс	Преподаватель-ский стол; столы обучающихся; стулья; классная доска; мультиме-дийный комплекс; ПК преподавате-ля; ПК обучаю-щихся; наглядные пособия (плакаты) *Место, оборудо-ванное для лиц с ограниченными возможностями.* Лицензионное программное обеспечение, под-ключенное к сети Интернет	1. 7-Zip (Бесплатное ПО); 2. 10-Strike Network Inventory ПО РФ (ПО) 3. Duductor Academic ПО РФ (Бесплатное ПО); https://basegroup.ru/deductor/manual/licence-deductor-academic 4. Eset Endpoint security (Платное ПО) https://help.eset.com/eula/ GIMP (Бесплатное ПО); https://docs.gimp.org/2.10/ru/ 5. microsoft office профессиональный плюс 2016 (ПО) https://www.microsoft.com/en-us/Useterms/Retail/Office/2016Professional/Useterms_Retail_Office_2016Professional_RUS.htm 6. Microsoft power Bi (Бесплатное ПО); https://powerbi.microsoft.com/ru-ru/windows-license-terms/ icrosoft Visual Studio (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mt171584/ 7. Notepad ++ (Бесплатное ПО); https://www.gnu.org/licenses/old-licenses/gpl-2.0.html 8. Zoom (Бесплатное ПО); https://explore.zoom.us/ru/terms/ 9. Anaconda3 2019 (Бесплатное ПО); 10. https://www.anaconda.com/eula-anaconda-individual-edition Android studio (Бесплатное ПО); https://developer.android.com/studio/terms 11. Brackets (Бесплатное ПО); https://github.com/brackets-cont/brackets/blob/master/LICENSE 12. CodeBlocks (Бесплатное ПО);https://www.codeblocks.org/license/ Firebird (Бесплатное ПО); https://firebirdsql.org/en/licensing/ 13. KNIME analytics platform (Бесплатное ПО); https://www.knime.com/downloads/full-license 14. Loginom community РФ ПО (Бесплатное ПО);https://loginom.ru/legal 15. Monogame SDK (Бесплатное ПО); https://github.com/MonoGame/MonoGame/blob/develop/LICENSE.txt Openproj (Бесплатное ПО); https://opensource.org/licenses/CPAL-1.0 16. tableau 2019 (Бесплатное ПО); https://www.tableau.com/legal 17. Visual studio community 2017 (Бесплатное ПО); https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-qZeRxv7zAhXhsYsKHZoRBAsQFnoECBgQAQ&url=https%3A%2F%2Fvisualstudio.microsoft.com%2Fwp-con-tent%2Fuploads%2F2017%2F01%2FVS2017_COMMUNITY_RC_RUS_Eula.1049-1.docx&usg=AOvVaw0tLxlQA4E2McNypfRn9tTo 18. Visual studio community 2019 (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mlt110718/ 19. Консультант плюс
3	Учебные аудитории для проведения занятий семи-нарского типа, курсового проектирова-ния (выполне-ния курсовых работ), груп-повых и инди-видуальных консультаций, текущего кон-	Преподаватель-ский стол; столы обучающихся; стулья; классная доска; мультиме-дийный комплекс; ПК преподавате-ля; ПК обучаю-щихся; наглядные пособия (плакаты) *Место, оборудо-ванное для лиц с ограниченными возможностями.*	1. 7-Zip (Бесплатное ПО); 2. 10-Strike Network Inventory ПО РФ (ПО) 3. Duductor Academic ПО РФ (Бесплатное ПО); https://basegroup.ru/deductor/manual/licence-deductor-academic 4. Eset Endpoint security (Платное ПО) https://help.eset.com/eula/ GIMP (Бесплатное ПО); https://docs.gimp.org/2.10/ru/ 5. microsoft office профессиональный плюс 2016 (ПО) https://www.microsoft.com/en-us/Useterms/Retail/Office/2016Professional/Useterms_Retail_Office_2016Professional_RUS.htm 6. Microsoft power Bi (Бесплатное ПО); https://powerbi.microsoft.com/ru-ru/windows-license-terms/ icrosoft Visual Studio (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mt171584/

	троля и промежуточной аттестации, а также самостоятельной работы обучающихся	Лицензионное программное обеспечение, подключенное к сети Интернет	7. Notepad ++ (Бесплатное ПО); https://www.gnu.org/licenses/old-licenses/gpl-2.0.html 8. Zoom (Бесплатное ПО); https://explore.zoom.us/ru/terms/ 9. Anaconda3 2019 (Бесплатное ПО); 10. https://www.anaconda.com/eula-anaconda-individual-edition Android studio (Бесплатное ПО); https://developer.android.com/studio/terms 11. Brackets (Бесплатное ПО); https://github.com/brackets-cont/brackets/blob/master/LICENSE 12. CodeBlocks (Бесплатное ПО);https://www.codeblocks.org/license/ Firebird (Бесплатное ПО); https://firebirdsql.org/en/licensing/ 13. KNIME analytics platform (Бесплатное ПО); https://www.knime.com/downloads/full-license 14. Loginom community РФ ПО (Бесплатное ПО);https://loginom.ru/legal 15. Monogame SDK (Бесплатное ПО); https://github.com/MonoGame/MonoGame/blob/develop/LICENSE.txt Openproj (Бесплатное ПО); https://opensource.org/licenses/CPAL-1.0 16. tableau 2019 (Бесплатное ПО); https://www.tableau.com/legal 17. Visual studio community 2017 (Бесплатное ПО); https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-qZeRxv7zAhXhsYsKHZoRBAsQFnoECBgQAQ&url=https%3A%2F%2Fvisualstudio.microsoft.com%2Fwp-con-tent%2Fuploads%2F2017%2F01%2FVS2017_COMMUNITY_RC_RUS_Eula.1049-1.docx&usg=AOvVaw0tLxlQA4E2McNypfRn9tTo 18. Visual studio community 2019 (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mlt110718/ 19. Консультант плюс
4	Библиотека с читальным залом	Стол обучающегося, стулья, ПК обучающегося, принтер Электронная библиотечная система и библиотечное абонентное обслуживание (учебная литература на бумажных носителях) Лицензионное программное обеспечение, подключенное к сети Интернет	1. 7-Zip (Бесплатное ПО); 2. microsoft office проффесиональный плюс 2016 (ПО) https://www.microsoft.com/en-us/Useterms/Retail/Office/2016Professional/Useterms_Retail_Office_2016Professional_RUS.htm 3. Microsoft power Bi (Бесплатное ПО); https://powerbi.microsoft.com/ru-ru/windows-license-terms/ icrosoft Visual Studio (Бесплатное ПО); https://visualstudio.microsoft.com/ru/license-terms/mt171584/ 4. Антиплагиат 5. Консультант плюс

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

8.1. Основная литература, в том числе электронные издания

1. Басыня Е.А. Сетевая информационная безопасность: учебник / Е.А. Басыня. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/132693.html (дата обращения: 06.07.2023). — Режим доступа: для авторизир. пользователей

2. Киренберг А.Г. Информационная безопасность современных операционных систем: учебное пособие / А.Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/128393.html (дата обращения: 21.02.2023). — Режим доступа: для авторизир. пользователей

8.2. Дополнительная литература, в том числе электронные издания

1. Куликов С.С. Информационная безопасность локальных компьютерных сетей: практикум / С.С. Куликов. — Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/118614.html (дата обращения: 29.06.2023). — Режим доступа: для авторизир. пользователей
2. Ревнивых А.В. Информационная безопасность в организациях: учебное пособие / А.В. Ревнивых. — Москва: Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/108227.html (дата обращения: 29.08.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/108227

8.3. Интернет-ресурсы:

- **Сайт ОЧУ ВО «Еврейский университет» https:// www.j-univer.ru/**
- **ЭБС IPR Books http://iprbookshop.ru** (учебники и учебные пособия, монографии, сборники научных трудов, научная периодика, профильные журналы, справочники, энциклопедии);
- **ООО «ИВИС» https://dlib.eastview.com (**электронные версии периодических изданий ООО «ИВИС»);
- **Web of Science http://webofknowledge.com/** (обширная международная универсальная реферативная база данных);
- **Scopus https://www.scopus.com** (международная универсальная реферативная база данных, индексирующая более 21 тыс. наименований научно-технических, гуманитарных и медицинских журналов, материалов конференций примерно 5000 международных издательств);
- **Научная электронная библиотека eLIBRARY.RU https://elibrary.ru** (крупнейший российский информационный портал в области науки, технологии, медицины и образования);
- **ООО «Национальная электронная библиотека» (НЭБ) http://нэб.рф/** (объединенные фонды публичных библиотек России федерального, регионального, муниципального уровня, библиотек научных и образовательных учреждений;
- **«НЭИКОН» http://www.neicon.ru/ (**доступ к современной зарубежной и отечественной научной периодической информации по гуманитарным и естественным наукам в электронной форме);
- **«Polpred.com Обзор СМИ» http://www.polpred.com (**статьи, интервью и др. информагентств и деловой прессы за 15 лет);
- **http://ecsocman.hse.ru** Федеральный образовательный портал «Экономика Социология Менеджмент»;
- Образовательный портал - https://e.muiv.ru/ на платформе «**Moodle**»

9. Перечень информационных технологий

Образовательный процесс по дисциплине поддерживается средствами электронной информационно-образовательной среды Университета, которая обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочей программе, через личный кабинет студента и преподавателя;
- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;
- проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением дистанционных образовательных технологий;
- формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;

- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети Интернет.

Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (ЭБС университета), содержащей издания учебной, учебно-методической и иной литературы по основным изучаемым дисциплинам и сформированной на основании прямых договоров с правообладателями.

Программное обеспечение, в т.ч. отечественного производства:

1. Adobe flash player 31;
2. Adobe reader 10;
3. Java 6.0;
4. K-Lite Codec Pack;
5. Win rar;
6. Microsoft Office 10;
7. Microsoft Visio 10;
8. Microsoft Visual studio.

Профессиональные базы данных и информационно-справочные системы:

1. Kaspersky Endpoint Security для бизнеса http://inion.ru/resources/bazy-dannykh-inion-ran/ - библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам;
2. http://www.scopus.com/ - реферативная база данных Scopus – международная универсальная реферативная база данных;
3. www.sostav.ru, База данных аналитических, исследовательских материалов по проблемам маркетинга и рекламы;
4. http://elibrary.ru/defaultx.asp - крупнейший российский информационный портал электронных журналов и баз данных по всем отраслям наук.
5. http://www.consultant.ru, справочная правовая система «Консультант Плюс».

10. Методические указания для обучающихся

10.1. Преподавание дисциплины осуществляется в соответствии с Федеральным государственным образовательным стандартом высшего образования

Основными формами получения и закрепления знаний по данной дисциплине являются занятия лекционного и семинарского типа, самостоятельная работа обучающегося, в том числе под руководством преподавателя, прохождение рубежного контроля.

Основной объем часов по изучению дисциплины согласно учебным планам приходится на самостоятельную работу обучающихся. Самостоятельная работа включает в себя изучение учебной, учебно-методической и специальной литературы, её конспектирование, подготовку к занятиям семинарского типа, текущему контролю и промежуточной аттестации (зачету или (и) экзамену).

Текущий контроль успеваемости по учебной дисциплине и промежуточная аттестация осуществляются в соответствие с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования: программам бакалавриата, программам специалитета, программам магистратуры.

Наличие в Университете электронной информационно-образовательной среды, а также электронных образовательных ресурсов позволяет осваивать курс инвалидам и лицам с ОВЗ.

10.2. Особенности освоения учебной дисциплины инвалидами и лицами с ограниченными возможностями здоровья

Особенности освоения учебной дисциплины инвалидами и лицами с ОВЗ определены в Положении об организации обучения студентов-инвалидов и студентов с ограниченными возможностями здоровья, утвержденным приказом ректора.

Обучение инвалидов и лиц с ОВЗ может осуществляться индивидуально, а также с примене-

нием электронного обучения, дистанционных образовательных технологий.
Выбор методов и средств обучения, образовательных технологий и учебно-методического обеспечения реализации образовательной программы осуществляется Университетом самостоятельно, исходя из необходимости достижения обучающимися планируемых результатов освоения образовательной программы, а также с учетом индивидуальных возможностей обучающихся из числа инвалидов и лиц с ОВЗ.
Форма проведения промежуточной аттестации для студентов-инвалидов и лиц с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости инвалидам и лицам с ОВЗ предоставляется дополнительное время для подготовки ответа на зачете или экзамене.
В группах, в состав которых входят студенты с ОВЗ, с целью реализации индивидуального подхода, а также принципа индивидуализации и дифференциации, рекомендуется использовать технологию нелинейной конструкции учебных занятий, предусматривающую одновременное сочетание фронтальных, групповых и индивидуальных форм работы с различными категориями студентов, в т.ч. имеющих ОВЗ.
В случае наличия обучающихся с нарушением функций опорно-двигательного аппарата, зрения и слуха, они обеспечиваются необходимым оборудованием, имеющимся в Университете, а также предоставляемым в рамках Соглашения с РУМЦ РГСУ от 14 ноября 2019 года.

11. Методические рекомендации преподавателю по организации учебного процесса по дисциплине

При изучении дисциплины рекомендуется использовать следующий набор средств и способов обучения:
– рекомендуемую основную и дополнительную литературу;
– задания для подготовки к занятиям семинарского типа (вопросы для обсуждения, кейс задания, расчетные задачи и др.);
– задания для текущего контроля успеваемости (задания для самостоятельной работы обучающихся, тестовые задания в рамках электронной системы тестирования);
– вопросы и задания для подготовки к промежуточной аттестации по итогам освоения дисциплины, позволяющие оценить знания, умения и уровень приобретенных компетенций.
При проведении занятий лекционного и семинарского типа, в том числе в форме вебинаров и on-line курсов необходимо строго придерживаться тематического плана дисциплины, приведенного в РПД. Необходимо уделить внимание рассмотрению вопросов и заданий, включенных в тестовые оценочные задания, при необходимости, решить аналогичные задачи с объяснением алгоритма решения.
Следует обратить внимание обучающихся на то, что для успешной подготовки к текущему контролю (выполнению ОЗ) и промежуточной аттестации (зачету или экзамену) недостаточно прочитать рабочий учебник, размещенный в личном кабинете. Нужно изучить материалы основной и дополнительной литературы, список которой приведен в РПД, законодательные и нормативные акты, а также материалы, рекомендованные в разделе «Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».
Текущий контроль успеваемости по учебной дисциплине и промежуточная аттестация осуществляются в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования: программам бакалавриата, программам специалитета, программам магистратуры.

Программа разработана Елагиной А.С.
Рабочая программа дисциплины рассмотрена и принята на заседании кафедры от 28.08.2023 г., протокол №1.

Лист регистрации изменений и дополнений
в рабочую учебную программу

Составителем внесены следующие изменения:

Содержание изменений	**Номер протокола и дата заседания кафедры по утверждению изменений**