ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Юридический институт

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Титова Е. В.
Пользователь: titovaev
Дата подписания: 07.11.2021

Е. В. Титова

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.11 Основы информационной безопасности в профессиональной деятельности
для специальности 40.05.01 Правовое обеспечение национальной безопасности
уровень специалист **тип программы** Специалитет
специализация Уголовно-правовая
форма обучения очная
кафедра-разработчик Конституционное и административное право

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 40.05.01 Правовое обеспечение национальной безопасности, утверждённым приказом Минобрнауки от 19.12.2016 № 1614

Зав.кафедрой разработчика,
к.юрид.н., доц.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Титова Е. В.
Пользователь: titovaev
Дата подписания: 07.11.2021

Е. В. Титова

Разработчик программы,
преподаватель (-)

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Мамаев В. В.
Пользователь: vvmamaev
Дата подписания: 07.11.2021

В. В. Мамаев

СОГЛАСОВАНО

Зав.выпускающей кафедрой
Уголовное и уголовно-исполнительное право, криминология
д.юрид.н., доц.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Дмитриева А. А.
Пользователь: dmitrievaaa
Дата подписания: 07.11.2021

А. А. Дмитриева

Челябинск

1. Цели и задачи дисциплины

Цели: ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами РФ. Задачи: - приобретение студентами теоретических знаний и практических навыков защиты информации представленной в электронном виде, прежде всего средствами криптографии, типичными криптосистемами и другими методами, лежащими в ее основе; - получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации; - формирование у студентов навыков защиты информации в локальных и глобальных компьютерных сетях.

Краткое содержание дисциплины

В программу включены темы, связанные с изучением доктрины информационной безопасности Российской Федерации, национальными интересами в информационной сфере и их обеспечением, концептуальной модели информационной безопасности, а также видами и источниками угроз информационной безопасности и направлениями обеспечения информационной безопасности. Рассматриваются правовое, организационное и инженерно-техническое обеспечения информационной безопасности, основные угрозы и стратегии защиты компьютерной информации, криптографические методы защиты данных, антивирусная защита компьютеров; методы и средства получения информации в локальных и глобальных компьютерных сетях, анализ конфигурации персонального компьютера, поиск информации с помощью специальных шаблонов и масок; организационно-технические аспекты получения и передачи компьютерной информации, компьютерные преступления.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Знать:основные понятия и определения, используемые при изучении информационной безопасности; классификацию угроз информационной безопасности; классические и современные методы взлома сетевых носителей и систем; классификацию компьютерных вирусов, какую угрозу они представляют для безопасности информации и правила защиты от компьютерных вирусов и вредоносных программ; как организовать информационную безопасность в организации; нормы и требования российского законодательства в области защиты информации.
	Уметь:правильно выбирать и использовать антивирусную защиту; восстанавливать пораженные компьютерными вирусами объекты средствами выбранной антивирусной защиты;

	осуществлять профессиональную деятельность с использованием информационно-правовых системам и иного программного обеспечения в сети Internet с соблюдением требований информационной безопасности.
	Владеть:навыками подбора и применения современных методов и способов защиты информации; работы с нормативными документами России в области защиты информации и обеспечения ее конфиденциальности; обеспечения соблюдения требований законодательства РФ о защите персональных данных.
ПК-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	Знать:основные понятия и определения в области информационной безопасности; классические и современные методы обработки информации в ходе оформления процессуальной и служебной документации; нормы и требования российского законодательства в области защиты информации.
	Уметь:правильно выбирать и использовать программное обеспечение прикладного характера и специального назначения для сбора, хранения, передачи и обработки процессуальной и служебной документации.
	Владеть:навыками подбора и применения современных методов и способов обработки информации в соответствии с нормативными документами России в области защиты информации и обеспечения ее конфиденциальности; обеспечения соблюдения требований законодательства РФ о защите персональных данных.
ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Знать:основные понятия и концепции современных технологий защиты информации; основные методы создания систем защиты информации; основные стандарты в области информационной безопасности; основные инструментальные средства защиты информации; источники возникновения информационных угроз; модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации.
	Уметь:анализировать типы атак и угроз информационной безопасности; формулировать соответствующие требования к системам защиты информации; применять правовые, организационные, технические и программные средства защиты информации.
	Владеть:базовыми навыками построения и управления систем защиты информации; навыками отражения типовых атак на информационные системы; базовыми навыками безопасной работы в компьютерных сетях при

	сборе, передаче и преобразовании информации; методами антивирусной защиты технических средств обработки информации.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.10 Информатика, Б.1.09 Математика, ДВ.1.02.01 Информационные технологии в профессиональной деятельности	В.1.06 Практикум по виду профессиональной деятельности, В.1.16 Государственная и муниципальная служба

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.09 Математика	Знать: основные понятия и методы математических рассуждений; роль и место математики структуре прикладных наук. Уметь: выполнять математические расчеты, применять формулы; уметь переводить и формулировать проблемы на математический язык из других не математических областей и использовать преимущество математики в их решении; уметь читать и проводить анализ математической литературы; уметь предоставлять математические утверждения и доказывать их в письменной и устной форме. Владеть: навыками формализации высказываний естественного языка и построения логических цепочек преобразования формализованных высказываний, методами и средствами математических доказательств при решении прикладных задач.
Б.1.10 Информатика	Знать: основы теории информации и кодирования, свойства информации, методы сбора, хранения, передачи и преобразования информации, технические и программные средства обработки информации. Уметь: создавать, хранить, структурировать и обрабатывать информацию с помощью современных технических устройств и комплексов. Владеть: практическими навыками работы с компьютером, как основным средством сбора, обработки, преобразования, хранения и передачи информации.
ДВ.1.02.01 Информационные технологии в профессиональной деятельности	Знать: информационные ресурсы и технологии сбора, хранения и обработки информации. Нормативные документы в области информатизации, хранения и обработки персональных данных. Уметь: пользоваться различными информационными ресурсами и

	технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации. Владеть: навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности; навыками эффективного использования современных справочно-информационных правовых систем.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	72	72
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	40	40
Изучение и анализ нормативно-правовой базы по темам с дальнейшим представлением информации на контактных занятиях	20	20
Подготовка к зачету	4	4
Поиск информации и подготовка сообщения по темам	16	16
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение в информационную безопасность	2	2	0	0
2	Правовое обеспечение информационной безопасности	4	2	2	0
3	Организационное обеспечение информационной безопасности	4	2	2	0
4	Механизмы обеспечения "информационной безопасности"	4	2	2	0
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	4	2	2	0
6	Криптографические методы защиты информации	4	2	2	0
7	Компьютерные вирусы и методы антивирусной защиты	6	2	4	0
8	Информационная безопасность вычислительных сетей	4	2	2	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации	2
2	2	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны	2
3	3	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия	2
4	4	Инженерная защита объектов. Защита информации от утечки по техническим каналам	2
5	5	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз	2
6	6	Системы шифрования. Цифровые подписи (ЭЦП). Инфраструктура открытых ключей. Криптографические протоколы	2
7	7	Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Антивирусные программы. Правила защиты от компьютерных вирусов.	2
8	8	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Адресация в глобальных сетях.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	2
2	3	Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности	2
3	4	Технические средства и методы защиты информации	2
4	5	Программные средства обеспечения информационной безопасности	2
5	6	Криптография и шифрование. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Механизм электронной цифровой подписи	2
6	7	Компьютерные вирусы и информационная безопасность. Классификация компьютерных вирусов. Методы обнаружения компьютерных вирусов. Изучение настроек средств антивирусной защиты информации	2
7	7	Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Методы профилактики заражения технических устройств и носителей компьютерными вирусами	2
8	8	Особенности обеспечения информационной безопасности в компьютерных сетях. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Адресация в глобальных сетях. Система доменных имен	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение и анализ информации по теме: "Защита интеллектуальной собственности средствами патентного и авторского права"	ЭУМД, осн. лит. №4, статья 14, статья 15, справочно-правовая система по законодательству Российской Федерации	8
Поиск, изучение и анализ информации по теме: "Теоретические основы аутентификации"	ЭУМД, доп. лит. №3, глава 3	8
Подготовка к зачёту	ЭУМД, осн лит. №4 статья 10.1, ЭУМД, осн. лит. №6 пункт 3, осн. лит. №7 статья 10.4, ЭУМД, доп. лит. глава 2	4
Поиск информации по теме: "Угрозы безопасности технических средств обработки информации"	ЭУМД, осн лит. №4 статья 10.1, ЭУМД, осн. лит. №6 пункт 3, осн. лит. №7 статья 10.4, ЭУМД, доп. лит. глава 2	4
Изучение нормативно-правовой базы по защите персональных данных	ЭУМД, осн. лит. №5, глава 1-5	10
Поиск информации по теме: "Концепции обеспечения информационной безопасности"	ЭУМД, осн. лит. №8, глава 1, ЭУМД, доп. лит. №3, глава 2, справочно-правовая система по законодательству Российской Федерации	6

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проблемно-ориентированное обучение	Лекции	Лекция-визуализация способствует созданию проблемной ситуации, разрешение которой, в отличие от классической проблемной лекции, где используются вопросы, происходит на основе анализа, синтеза, обобщения, свертывания или развертывания информации, то есть с включением активной мыслительной деятельности. Основная задача преподавателя - использовать такие формы наглядности, которые не только дополняли словесную информацию, но и сами являлись носителями информации. Чем больше проблемности в наглядной информации, тем выше степень мыслительной активности студента. Методика проведения подобной лекции предполагает предварительную подготовку визуальных материалов в соответствии с ее содержанием. Подготовка лекции преподавателем состоит в том, чтобы изменить, переконструировать учебную информацию (всю или часть на его усмотрение, исходя из методической необходимости) по теме лекционного занятия в визуальную форму для представления студентам через технические средства обучения или вручную: схемы, рисунки, чертежи и т. п. "Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации", "Основные	16

		нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны", "Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия", "Инженерная защита объектов. Защита информации от утечки по техническим каналам", "Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз", "Системы шифрования. Цифровые подписи (ЭЦП). Инфраструктура открытых ключей. Криптографические протоколы", "Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Антивирусные программы. Правила защиты от компьютерных вирусов", "Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Адресация в глобальных сетях"	
Личностно-ориентированное обучение	Практические занятия и семинары	Личностно ориентированное занятие в отличие от традиционного в первую очередь изменяет тип взаимодействия «преподаватель-студент». От командного стиля педагог переходит к сотрудничеству, ориентируясь на анализ не столько результатов, сколько процессуальной деятельности обучаемого. Изменяются позиции студента – от прилежного исполнения к активному творчеству, иным становится его мышление: рефлексивным, то есть нацеленным на результат. Меняется и характер складывающихся на занятии отношений. Главное же в том, что преподаватель не только дает знания, но и создает оптимальные условия для развития личности студента ("Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности", "Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности", "Технические средства и методы защиты информации", "Программные средства обеспечения информационной безопасности", "Криптография и шифрование. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Механизм электронной цифровой подписи", "Компьютерные вирусы и информационная безопасность. Классификация компьютерных вирусов. Методы обнаружения компьютерных вирусов. Изучение настроек средств антивирусной защиты информации", "Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Методы профилактики заражения технических устройств и носителей компьютерными вирусами", "Особенности обеспечения информационной безопасности в компьютерных	16

		сетях. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Адресация в глобальных сетях. Система доменных имен")	

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Проведение лекций-визуализаций с применением интерактивных методов обучения	Вся информация сопровождается наглядным представлением материала (электронные презентации), используются методы опережающего обучения с обязательным выполнением домашних творческих заданий, подготовкой докладов и сообщений по поставленной проблематике
Проведение практических занятий с применением элементов личностно-ориентированного обучения	Планирование практических занятий позволяющих посредством опоры на систему взаимосвязанных понятий, идей и способов действий обеспечить и поддержать процессы самопознания, самореализации личности каждого студента, развитие его неповторимой индивидуальности и повышение уровня его самооценки

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Введение в информационную безопасность	ПК-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	Выполнение творческих заданий	Задание №№1. Перечень тем для самостоятельной подготовки №1
Правовое обеспечение информационной безопасности	ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Выполнение творческих заданий	Задания №№2-3. Перечень тем для самостоятельной подготовки №1
Организационное обеспечение информационной безопасности	ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Выполнение практических заданий	Задания №№1-2. Блок заданий №1

Механизмы обеспечения "информационной безопасности"	ПК-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	Выполнение творческих заданий	Задания №№1,2. Тематика докладов №2
Программно-аппаратные средства и методы обеспечения информационной безопасности	ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Выполнение практических заданий	Задания №№3-4. Блок заданий №1
Криптографические методы защиты информации	ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Выполнение практических заданий	Задания №№5-6. Блок заданий №2
Информационная безопасность вычислительных сетей	ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Выполнение творческих заданий	Задания №№1-3. Тематика заданий №5
Информационная безопасность вычислительных сетей	ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Выполнение практических заданий	Задания №№7-8. Блок заданий №2
Все разделы	ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Мероприятия текущей аттестации (итоговое тестирование)	Компьютерное тестирование
Все разделы	ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Мероприятия текущей аттестации (тестирование)	Компьютерное тестирование
Все разделы	ПК-13 способностью правильно и полно отражать результаты	Мероприятия текущей	Компьютерное тестирование

	профессиональной деятельности в процессуальной и служебной документации	аттестации (тестирование)	
Все разделы	ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Зачет	Задания контрольно-рейтинговых мероприятий текущего контроля и промежуточной аттестации
Все разделы	ПК-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	Зачет	Задания контрольно-рейтинговых мероприятий текущего контроля и промежуточной аттестации
Все разделы	ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Зачет	Задания контрольно-рейтинговых мероприятий текущего контроля и промежуточной аттестации

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Выполнение творческих заданий	Проверка выполнения творческих заданий осуществляется 2 раза в семестр перед аттестацией. Студентам предлагается выполнить 10 творческих заданий за семестр (5 до первой аттестации, 5 до второй аттестации). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучаемого (утверждена приказом ректора от 24.05.2019 г. №179). Творческое задание должно быть выполнено с использованием современных информационных технологий и представлено в виде электронной презентации для обсуждения на контактном занятии лекции-обсуждении. Задание выполнено в полном объеме и студент выступил с презентацией - 2 балла; Задание выполнено в полном объеме, но без представления на перед аудиторией - 1 балл; Задание не выполнено - 0 баллов. Максимальное количество баллов за каждый перечень заданий - 10 баллов. Весовой коэффициент (за каждый перечень творческих заданий) - 0,1.	Зачтено: Рейтинг обучаемого за мероприятие больше или равен 60% Не зачтено: Рейтинг обучаемого за мероприятие менее 60%
Выполнение практических заданий	Оценка выполнения практических заданий осуществляется 2 раза в семестр перед аттестацией. Студентам предлагается выполнить 8 практических заданий за семестр (4 из первого блока - до первой аттестации, 4 из второго блока - до второй аттестации). При оценивании результатов мероприятия используется	Зачтено: Рейтинг обучающегося за мероприятие больше либо равен 60% Не зачтено: Рейтинг обучающегося за

	балльно-рейтинговая система оценивания результатов учебной деятельности обучаемого (утверждена приказом ректора от 24.05.2019 г. №179). Практические задания должны быть выполнены в соответствии с методическими указаниями и представлены в электронном виде. Задание выполнено в полном объеме, без замечаний оценивается в 1 балл; задание выполнено частично, либо с замечаниями - оценивается в 0,5 баллов; задание не выполнено либо не представлено на проверку в электронном виде - оценивается в 0 баллов. Максимальное количество баллов за каждый этап выполнения практических заданий (перед каждой аттестацией) - 10 баллов. Весовой коэффициент (за каждые 10 практических заданий) - 0,2.	мероприятие менее 60%
Мероприятия текущей аттестации (тестирование)	Промежуточная аттестация включает компьютерное тестирование. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучаемого (утверждена приказом ректора от 24.05.2019 г. №179). Тест состоит из 20 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 60 минут. Правильный ответ на вопрос соответствует 2 баламу. Неправильный ответ на вопрос соответствует 0 баллов. Максимальное количество баллов за промежуточную аттестацию - 40. Весовой коэффициент - 0,4	Зачтено: Рейтинг обучающегося за мероприятие больше либо равен 60% Не зачтено: Рейтинг обучающегося за мероприятие менее 60%
Зачет	На зачете происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. Студент вправе прийти на зачет для улучшения своего рейтинга и получить оценку с учетом текущего рейтинга и баллов за промежуточное испытание. Для этого он проходит испытание промежуточной аттестации в форме компьютерного тестирования. Тест состоит из 20 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 60 минут. Правильный ответ на вопрос соответствует 2 баллам. Неправильному ответу на вопрос соответствует 0 баллов. Максимальное количество баллов - 40. Весовой коэффициент мероприятия - 0,4. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучаемого (утверждена приказом ректора от 24.05.2019 г. №179).	Зачтено: Рейтинг обучающегося больше или равен 60% Не зачтено: Рейтинг обучающегося за мероприятие менее 60%

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Выполнение творческих заданий	Подготовить сообщение по предложенным темам: 1. Информационная безопасность. Основные понятия. 2. Модели информационной безопасности. 3. Виды защищаемой информации. Тематика творческих заданий 1. Что такое криптография. Какие используются симметричные алгоритмы

	шифрования? Какие используются ассиметричные алгоритмы шифрования? 2. Что такое криптографическая хеш-функция? Какие используются криптографические хеш-функции? 3. Что такое цифровая подпись? Что такое инфраструктура открытых ключей? Какие российские и международные стандарты на формирование цифровой подписи существуют? Задания 1. Докажите, что в современном обществе все большую актуальность приобретает знание нравственно-этических норм и правовых основ использования средств новых информационных технологий в повседневной практической деятельности. 2. Приведите примеры, иллюстрирующие рост борьбы с нарушениями нравственных и правовых норм в сфере информационной безопасности. 3. Проанализируйте состояние информационной безопасности в компьютерном классе Вашего учебного заведения. Предложите дополнительные мероприятия по повышению уровня информационной безопасности. 4. Приведите примеры из жизни, из кино- и видеофильмов, иллюстрирующие использование уязвимых мест и нарушения мер защиты информационной безопасности для несанкционированного проникновения в охраняемые системы. 5. Проведите анализ использования магнитных носителей в компьютерном классе Вашего учебного заведения с точки зрения обеспечения норм информационной безопасности, сформулируйте предложения по укреплению информационной безопасности кабинета. №1. Перечень тем для самостоятельной подготовки.pdf; №5. Тематика заданий.pdf; №2. Тематика докладов.pdf; №6. Задания.pdf
Выполнение практических заданий	Поиск информации по теме: "Концепции обеспечения информационной безопасности" Вопросы по теме: «Введение в информационную безопасность» 1. Что такое информационная безопасность? 2. Перечислите основные угрозы информационной безопасности. 3. Какие существуют модели информационной безопасности? 4. Какие методы защиты информации выделяют? 5. Что такое правовые методы защиты информации? Блок 2.pdf; Блок 1.pdf
Мероприятия текущей аттестации (тестирование)	Тестовые задания по теме «Концепции обеспечения информационной безопасности» 1. Что такое организационные методы защиты информации? 2. Что такое технические методы защиты информации? 3. Что такое программно-аппаратные методы защиты информации? 4. Что такое криптографические методы защиты информации? 5. Что такое физические методы защиты информации? 6. Какие главные государственные органы в области обеспечения информационной безопасности? 7. Перечислите виды защищаемой информации. Примерные тестовые задания: В чем заключаются цели государства в области обеспечения информационной безопасности? 1. обеспечение доступности, целостности и конфиденциальности информации; 2. обеспечение информационной безопасности компьютерных сетей и защита прав пользователей; 3. обеспечение защиты от несанкционированного доступа к информационным ресурсам государства; 4. обеспечение доступа каждого гражданина государства ко всем

	информационным массивам данных. Что понимается под "компьютерной безопасностью"? 1. это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий в компьютерных сетях; 2. это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера; 3. это защищенность информации и поддерживающей ее инфраструктуры от преднамеренных воздействий естественного или искусственного характера в распределенных сетях; 4. это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера в сети Internet. №4. Контрольные вопросы по теме.pdf; №3. Контрольные вопросы по теме.pdf; Вопросы к зачету.pdf
Зачет	Тестовые задания по теме «Программно-аппаратные средства и методы обеспечения информационной безопасности» 1. Какие виды компьютерных угроз существуют? 2. Что такое брандмауэр? 3. Что такое антивирусная программа? 4. Что такое эвристический алгоритм поиска вирусов? 5. Что такое сигнатурный поиск вирусов? 6. Методы противодействия сниффингу? 7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете? 8. Что такое механизм контроля и разграничения доступа? 9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации? 10. Что такое средства стеганографической защиты информации? Примерные тестовые задания: На установление соответствия между понятиями (выбрать термин и соответствующее ему значение) Тестовые задания по теме «Концепции обеспечения информационной безопасности» 1. Что такое организационные методы защиты информации? 2. Что такое технические методы защиты информации? 3. Что такое программно-аппаратные методы защиты информации? 4. Что такое криптографические методы защиты информации? 5. Что такое физические методы защиты информации? 6. Какие главные государственные органы в области обеспечения информационной безопасности? 7. Перечислите виды защищаемой информации. Примерные тестовые задания: В чем заключаются цели государства в области обеспечения информационной безопасности? 1. обеспечение доступности, целостности и конфиденциальности информации; 2. обеспечение информационной безопасности компьютерных сетей и защита прав пользователей; 3. обеспечение защиты от несанкционированного доступа к информационным ресурсам государства; 4. обеспечение доступа каждого гражданина государства ко всем информационным массивам данных. Что понимается под "компьютерной безопасностью"? 1. это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий в компьютерных сетях;

	2. это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера; 3. это защищенность информации и поддерживающей ее инфраструктуры от преднамеренных воздействий естественного или искусственного характера в распределенных сетях; 4. это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера в сети Internet. Вопросы к зачету.pdf

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Закиров, Р. Ш. Информационная безопасность Текст конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Вестник УрФО : Безопасность в информационной сфере. - 2011. - № 1. - С. 71-75. Мигунова, П. А. Проблемы обеспечения безопасности персональных данных в органе исполнительной власти субъекта Российской Федерации, осуществляющем переданные полномочия в области содействия занятости населения [Текст] / П. А. Мигунова

г) методические указания для студентов по освоению дисциплины:

1. Компьютерные вирусы и антивирусная защита
2. Обмен информацией в глобальных и локальных сетях
3. Классификация программного обеспечения
4. Базовые технологии компьютерных сетей
5. Архиваторы

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Компьютерные вирусы и антивирусная защита
2. Обмен информацией в глобальных и локальных сетях
3. Классификация программного обеспечения
4. Базовые технологии компьютерных сетей
5. Архиваторы

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание

1	Основная литература	Электронная библиотека Юрайт	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968 (дата обращения: 01.11.2021).
2	Дополнительная литература	Электронная библиотека Юрайт	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469866 (дата обращения: 01.11.2021).
3	Дополнительная литература	Электронная библиотека Юрайт	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469235 (дата обращения: 01.11.2021).

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)
2. -База данных ВИНИТИ РАН(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	112 (8Э)	Компьютерный класс на 6 рабочих мест. Компьютеры конфигурации: Intel Celeron G3930 2.9 GHz \4Gb\500Gb. Дополнительно столов -2 на 14 мест. Всего посадочных мест-30. Окна – 3 шт. Входные двери -1 шт.
Лекции	206 (8Э)	Рабочее место преподавателя. Компьютер конфигурации: Pentium-915 2800/1024Mb/250G Устройства коммутации и усиления аудио и видеосигналов, звуковая система. Проектор BenQ, проекционный экран. парты аудиторные- 40 шт. Посадочных мест -160 Окна -7 шт. Вх. двери-2 шт.