ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Юридический институт

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: 10.11.2021

Е. В. Титова

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.11 Основы информационной безопасности в профессиональной деятельности
для специальности 40.05.02 Правоохранительная деятельность
уровень специалист **тип программы** Специалитет
специализация Административная деятельность
форма обучения заочная
кафедра-разработчик Конституционное и административное право

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 40.05.02 Правоохранительная деятельность, утверждённым приказом Минобрнауки от 16.11.2016 № 1424

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

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: 08.11.2021

Е. В. Титова

Разработчик программы,
преподаватель (-)

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: 08.11.2021

В. В. Мамаев

СОГЛАСОВАНО

Зав.выпускающей кафедрой
Правоохранительная
деятельность и национальная
безопасность
д.юрид.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зуев С. В.
Пользователь: zuevsv
Дата подписания: 10.11.2021

С. В. Зуев

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-22 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 в области информационной безопасности; классические и современные методы обработки и защиты информации в ходе оформления процессуальной и служебной документации; нормы и требования российского законодательства в области защиты информации и конфиденциальности данных.
	Уметь:правильно выбирать и использовать программное обеспечение прикладного характера и специального назначения для сбора, хранения, передачи и обработки процессуальной и служебной документации с целью обеспечения соблюдения режима секретности.
	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 и соблюдению режима секретности.
ПК-16 способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	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.
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, ДВ.1.02.01 Информационные технологии в профессиональной деятельности	Не предусмотрены

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

Дисциплина	Требования
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.
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.

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:	8	8
Лекции (Л)	4	4
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	4	4
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	64	64
Подготовка к зачёту	8	8
Поиск информации и подготовка сообщения по темам	32	32
Изучение и анализ нормативно-правовой базы по темам с дальнейшим представлением информации на контактных занятиях	24	24
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. Правовое обеспечение информационной безопасности	1	1	0	0
2	Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"	1	1	0	0
3	Программно-аппаратные средства и методы обеспечения информационной безопасности. Криптографические методы защиты информации.	4	1	3	0
4	Криптографические методы защиты информации. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей.	2	1	1	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. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.	1
1	2	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам.	1
2	3	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Системы шифрования. Цифровые подписи (ЭЦП). Инфраструктура открытых ключей. Криптографические протоколы.	1

2	4	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. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Адресация в глобальных сетях.	1

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	3	Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Технические средства и методы защиты информации. Программные средства обеспечения информационной безопасности.	2
1	3	Криптография и шифрование. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Механизм электронной цифровой подписи	1
2	4	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 сетях. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Адресация в глобальных сетях. Система доменных имен.	1

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
Поиск информации по теме: "Концепции обеспечения информационной безопасности"	ЭУМД, осн. лит. №5 глава 2, справочно-правовая система по законодательству Российской Федерации	10
Изучение и анализ информации по теме: "Защита интеллектуальной собственности средствами патентного и авторского права"	ЭУМД, осн. лит. №4, глава 4, справочно-правовая система по законодательству Российской Федерации	10
Поиск информации по теме: "Угрозы безопасности технических средств обработки информации"	ЭУМД, доп. лит. №1 тема 2, доп. лит. №2 раздел 3	12
Подготовка к зачету	ЭУМД, осн. лит. №3-5, доп. лит 1-2	8
Поиск, изучение и анализ информации по теме: "Теоретические основы аутентификации"	ЭУМД, осн. лит. №5 главы 11-12	10

Изучение нормативно-правовой базы по защите персональных данных	ЭУМД, доп. лит. №2 раздел 2, осн. лит. №5 глава 14	14

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проблемно-ориентированного обучения	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 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	4

		глобальных сетях"	
Личностно-ориентированного обучения	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 сетях. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Адресация в глобальных сетях. Система доменных имен")	4

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
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
Проведение лекций-визуализаций с применением интерактивных методов	Вся информация сопровождается наглядным представлением материала (электронные презентации), используются методы опережающего обучения с обязательным выполнением домашних

обучения	творческих заданий, подготовкой докладов и сообщений по поставленной проблематике

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-16 способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	Текущий: домашнее задание	1-3
Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"	ПК-22 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Текущий: доклад	1-2
Организационное обеспечение информационной безопасности	ПК-16 способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	Текущий: проверка выполнения домашнего задания	1
Криптографические методы защиты информации. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей.	ПК-22 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Текущий: ответы на контрольные вопросы	1-12
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	Текущий: контрольные вопросы по теме	1-10
Криптографические методы защиты информации	ПК-16 способностью реализовывать мероприятия по получению	Текущий: выполнение	1-3

	юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	творческого домашнего задания	
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	Текущий: выполнение практического задания	1-5
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	Текущий: письменный опрос	1-10
Все разделы	ПК-16 способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	Текущий: рейтинговая оценка	1-16
Все разделы	ПК-16 способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	Промежуточный: зачет	1-16
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	Промежуточный: зачет	1-30
Все разделы	ПК-22 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Промежуточный: зачет	1-30

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и	Критерии оценивания

	оценивания	
Текущий: домашнее задание	Представление информации в письменной форме	Зачтено: Представленная информация соответствует заданной тематике Не зачтено: Отсутствие представленной информации
Текущий: доклад	Устное представление информации	Зачтено: Устное либо письменное представление доклада, полнота и соответствие выбранной теме Не зачтено: Отсутствие доклада
Текущий: проверка выполнения домашнего задания	Устное представление информации	Зачтено: Выполненное домашнее задание Не зачтено: Отсутствие выполненного домашнего задания
Текущий: ответы на контрольные вопросы	Письменный опрос	Отлично: 96-100% правильных ответов Хорошо: 90-95% правильных ответов Удовлетворительно: 75-89% правильных ответов Неудовлетворительно: <75% правильных ответов
Текущий: контрольные вопросы по теме	Письменный опрос	Зачтено: 75-100% правильных ответов Не зачтено: <75% правильных ответов
Текущий: выполнение творческого домашнего задания	Письменное представление	Зачтено: Качество представленной информации, творческий подход (индивидуализация выбранного процесса), использование IT-технологий Не зачтено: Отсутствие представленной информации
Текущий: выполнение практического задания	Письменное представление	Зачтено: Соответствие представленных материалов теме, полнота и достоверность информации. наличие прмеров и собственного мнения Не зачтено: Отсутствие представленной информации
Текущий: рейтинговая оценка	Подсчет оценочных баллов по результатам выполнения заданий, определение рейтинговой позиции студента	Зачтено: Рейтинговая оценка: более, либо равна 480 баллов Не зачтено: Рейтинговая оценка: менее 480 баллов
Промежуточный: зачет	Устный опрос	Зачтено: Рейтинговая оценка: более, либо равна 480 баллов Не зачтено: Рейтинговая оценка: менее 480 баллов и отсутствие правильного ответа на вопрос
Промежуточный: зачет	Тестирование	Отлично: 91-100% правильных ответов Хорошо: 75-90% правильных ответов Удовлетворительно: 60-74% правильных ответов Неудовлетворительно: <60% правильных ответов

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Текущий: домашнее задание	Подготовить сообщение по предложенным темам: 1. Информационная безопасность. Основные понятия. 2. Модели информационной безопасности.

	3. Виды защищаемой информации. №1. Перечень тем для самостоятельной подготовки.pdf
Текущий: доклад	Выбрать тему доклада: 1. Основные нормативно-правовые акты в области информационной безопасности. 2. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны №2. Тематика докладов.pdf
Текущий: проверка выполнения домашнего задания	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?
Текущий: ответы на контрольные вопросы	Контрольные вопросы 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. №3. Контрольные вопросы по теме.pdf
Текущий: контрольные вопросы по теме	Контрольные вопросы 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? №4. Контрольные вопросы по теме.pdf
Текущий: выполнение творческого домашнего задания	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? №5. Тематика заданий.pdf
Текущий: выполнение практического задания	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. №6. Задания.pdf
Текущий: рейтинговая оценка	Перечень заданий и видов деятельности для комплексной рейтинговой оценки деятельности студентов Обязательное выполнение практических заданий по темам: 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности 2. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности 3. Технические средства и методы защиты информации 4. Программные средства обеспечения информационной безопасности 5. Криптография и шифрование. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Механизм электронной цифровой подписи 6. Компьютерные вирусы и информационная безопасность. Классификация компьютерных вирусов. Методы обнаружения компьютерных вирусов. Изучение настроек средств антивирусной защиты информации 7. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Методы профилактики заражения технических устройств и носителей компьютерными вирусами 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 Дополнительные задания 1. Поиск информации по теме: "Концепции обеспечения информационной безопасности" 2. Поиск информации по теме: "Угрозы безопасности технических средств обработки информации" 3. Изучение и анализ информации по теме: "Защита интеллектуальной собственности средствами патентного и авторского права" 4. Поиск, изучение и анализ информации по теме: "Теоретические основы аутентификации" 5. Изучение нормативно-правовой базы по защите персональных данных критерии бально-рейтинговой оценки.pdf
Промежуточный: зачет	Вопросы к зачету для оценки качества освоения учебной дисциплины 1. Цели государства в области обеспечения информационной безопасности.

	2. Основные нормативные акты РФ, связанные с правовой защитой информации. 3. Виды компьютерных преступлений. 4. Способы и механизмы совершения информационных компьютерных преступлений. 5. Основные параметры и черты информационной компьютерной преступности в России. 6. Компьютерный вирус. Основные виды компьютерных вирусов. 7. Методы защиты от компьютерных вирусов. 8. Типы антивирусных программ. 9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя. 10. Основные угрозы компьютерной безопасности при работе в сети Интернет. 11. Виды защищаемой информации. 12. Государственная тайна как особый вид защищаемой информации. 13. Конфиденциальная информация. 14. Система защиты государственной тайны. 15. Правовой режим защиты государственной тайны. 16. Защита интеллектуальной собственности средствами патентного и авторского права. 17. Международное законодательство в области защиты информации. 18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях. 19. Симметричные шифры. 20. Ассиметричные шифры. 21. Криптографические протоколы. 22. Криптографические хеш-функции. 23. Электронная подпись. 24. Организационное обеспечение информационной безопасности. 25. Служба безопасности организации. 26. Методы защиты информации от утечки в технических каналах. 27. Инженерная защита и охрана объектов. критерии бально-рейтинговой оценки.pdf; Вопросы к зачету.pdf
Промежуточный: зачет	Тестовые задания содержат вопросы по темам: "Вирусы и антивирусная защита", "Сети и обеспечение безопасности в локальных и глобальных сетях" 1. Компьютерный вирус - это … 2. Вирусы можно классифицировать по ... 3. Основными путями проникновения вирусов в компьютер являются... 4. Основные признаки проявления вирусов ... 5. Антивирусные программы - это программы для ... . 11. Централизованный контроль за работой сети осуществляется при топологии 12. Экономный расход кабеля при топологии 13. Репитеры используются при топологии 14. В текущее время по сети может проходить только одно сообщение при топологии 15. Сообщения «идут» во всех направлениях при топологи .... Примерные тесты по сетям.pdf; Примерные тесты по антивирусной защите информации.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. Обмен информацией в глобальных и локальных сетях
2. Базовые технологии компьютерных сетей
3. Архиваторы
4. Компьютерные вирусы и антивирусная защита
5. Классификация программного обеспечения

из них: учебно-методическое обеспечение самостоятельной работы студента:

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

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронная библиотека Юрайт	Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476294 (дата обращения: 02.11.2021).
2	Дополнительная литература	Электронная библиотека Юрайт	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 02.11.2021).

3	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: 02.11.2021).
4	Основная литература	Электронная библиотека Юрайт	Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476798 (дата обращения: 02.11.2021).
5	Основная литература	Электронная библиотека Юрайт	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469133 (дата обращения: 02.11.2021).

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 16 рабочих мест. Компьютеры конфигурации: Intel Celeron G3930 2.9 GHz \4Gb\500Gb. Проектор BenQ, проекционный экран Стол одноместный – 16шт. 2хместных столов – 10 шт. Всего посадочных мест-36. 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