

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: Беляева И. М.	
Пользователь: belyaevaaim	
Дата подписания: 17.12.2018	

И. М. Беляева

РАБОЧАЯ ПРОГРАММА к ОП ВО от 27.06.2018 №007-03-1965

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 Профессиональная подготовка и управление в правоохранительной сфере

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,
д.пед.н., доц.

3. Р. Танаева

ЮУрГУ	Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП	
Кому выдан: Танаева З. Р.	
Пользователь: tanaevazr	
Дата подписания: 11.12.2018	

Разработчик программы,
доцент

Е. И. Елизарова

ЮУрГУ	Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП	
Кому выдан: Елизарова Е. И.	
Пользователь: elizarovaei	
Дата подписания: 11.12.2018	

СОГЛАСОВАНО

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

И. М. Беляева

ЮУрГУ	Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП	
Кому выдан: Беляева И. М.	
Пользователь: belyaevaaim	
Дата подписания: 17.12.2018	

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 крипtosистемами 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)
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

	<p>средства защиты информации.</p> <p>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.</p>
ПК-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	<p>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.</p> <p>Уметь: правильно выбирать и использовать программное обеспечение прикладного характера и специального назначения для сбора, хранения, передачи и обработки процессуальной и служебной документации.</p>
	<p>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.</p>
ПК-16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	<p>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.</p> <p>Уметь: правильно выбирать и использовать антивирусную защиту; восстанавливать пораженные компьютерными вирусами объекты средствами выбранной антивирусной защиты; осуществлять профессиональную деятельность с использованием информационно-правовых систем и иного программного обеспечения в сети Internet с соблюдением требований информационной безопасности.</p>
	<p>Владеть: навыками подбора и применения современных методов и способов защиты информации; работы с нормативными документами России в области защиты информации и обеспечения ее</p>

конфиденциальности; обеспечения соблюдения требований законодательства РФ о защите персональных данных.

3. Место дисциплины в структуре ОП ВО

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

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

Дисциплина	Требования
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.
Б.1.09 Математика	Знать: основные понятия и методы математических рассуждений; роль и место математики в 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 представлять 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.
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	
<i>Аудиторные занятия:</i>			
Лекции (Л)	16	16	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	40	40	
Поиск информации и подготовка сообщения по темам	18	18	
Изучение и анализ нормативно-правовой базы по темам с дальнейшим представлением информации на контактных занятиях	22	22	
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
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
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 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	10
Поиск, изучение и анализ информации по теме: "Теоретические основы аутентификации"	ЭУМД, доп. лит. №3, глава 3	8
Изучение нормативно-правовой базы по защите персональных данных	ЭУМД, осн. лит. №5, глава 1-5	12

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
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	16

		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")	
Проблемно-ориентированное обучение	Лекции	<p>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.</p> <p>"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</p>	16

	передачи данных. Адресация в глобальных сетях"	
--	--	--

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	Текущий: домашнее задание	1-3
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	Текущий: доклад	1-2
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	Текущий: проверка выполнения домашнего задания	1
Механизмы обеспечения "информационной безопасности"	ПК-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	Текущий: ответы на контрольные вопросы	1-12
Программно-аппаратные средства и методы	ОК-12 способностью работать с различными информационными	Текущий: контрольные	1-10

обеспечения информационной безопасности	ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	вопросы по теме	
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	Текущий: выполнение творческого домашнего задания	1-3
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	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 соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Текущий: рейтинговая оценка	1-16
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	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-13 способностью правильно и полно отражать результаты профессиональной деятельности в процессуальной и служебной документации	Промежуточный: зачет	1-30

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии 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 ИТ-технологий Не зачтено: Отсутствие представленной информации
Текущий: выполнение практического задания	Письменное представление	Зачтено: Соответствие представленных материалов теме, полнота и достоверность информации. наличие примеров 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
Промежуточный: зачет	Подсчет оценочных баллов студентов по всем видам учебной деятельности в семестре и допуск к итоговому тестированию и опросу: 1. Выполнение аудиторных практических заданий: 0-100 баллов; 2. Выполнение дополнительных творческих заданий: 25, 50, 75, 100 баллов; 3. Отсутствие на лекционном контактном занятии: -25 баллов; 4. Отсутствие на практическом контактном занятии: -100 баллов.	Зачислено: К тестированию допускаются студенты, набравшие за семестр более 480 баллов Не зачислено: К тестированию не допускаются студенты, набравшие за семестр 480 баллов и менее

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?

	<p>5. Что такое сигнатурный поиск вирусов?</p> <p>6. Методы противодействия снiffингу?</p> <p>7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?</p> <p>8. Что такое механизм контроля и разграничения доступа?</p> <p>9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?</p> <p>10. Что такое средства стеганографической защиты информации?</p> <p>№4. Контрольные вопросы по теме.pdf</p>
Текущий: выполнение творческого домашнего задания	<p>Тематика творческих заданий</p> <p>1. Что такое криптография. Какие используются симметричные алгоритмы шифрования? Какие используются ассиметричные алгоритмы шифрования?</p> <p>2. Что такое криптографическая хеш-функция? Какие используются криптографические хеш-функции?</p> <p>3. Что такое цифровая подпись? Что такое инфраструктура открытых ключей? Какие российские и международные стандарты на формирование цифровой подписи существуют?</p> <p>№5. Тематика заданий.pdf</p>
Текущий: выполнение практического задания	<p>Задания</p> <p>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.</p> <p>2. Приведите примеры, иллюстрирующие рост борьбы с нарушениями нравственных и правовых норм в сфере информационной безопасности.</p> <p>3. Проанализируйте состояние информационной безопасности в компьютерном классе Вашего учебного заведения. Предложите дополнительные мероприятия по повышению уровня информационной безопасности.</p> <p>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.</p> <p>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.</p> <p>№6. Задания.pdf</p>
Текущий: рейтинговая оценка	<p>Перечень заданий и видов деятельности для комплексной рейтинговой оценки деятельности студентов</p> <p>Обязательное выполнение практических заданий по темам:</p> <p>1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности</p> <p>2. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности</p> <p>3. Технические средства и методы защиты информации</p> <p>4. Программные средства обеспечения информационной безопасности</p> <p>5. Криптография и шифрование. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Механизм электронной цифровой подписи</p> <p>6. Компьютерные вирусы и информационная безопасность. Классификация компьютерных вирусов. Методы обнаружения компьютерных вирусов. Изучение настроек средств антивирусной защиты информации</p> <p>7. Характеристика путей проникновения вирусов в компьютеры. Правила</p>

	<p>защиты от компьютерных вирусов. Методы профилактики заражения технических устройств и носителей компьютерными вирусами</p> <p>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</p> <p>Дополнительные задания</p> <ol style="list-style-type: none"> 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 балльно-рейтинговой оценки.pdf
Промежуточный: зачет	<p>Вопросы к зачету</p> <p>для оценки качества освоения</p> <p>учебной дисциплины</p> <ol style="list-style-type: none"> 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. <p>Вопросы к зачету.pdf</p>

	<p>Тестовые задания содержат вопросы по темам: "Вирусы и антивирусная защита", "Сети и обеспечение безопасности в локальных и глобальных сетях"</p> <ol style="list-style-type: none"> 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 ... <p>....</p>
Промежуточный: зачет	<p>11. Централизованный контроль за работой сети осуществляется при топологии</p> <p>12. Экономный расход кабеля при топологии</p> <p>13. Репитеры используются при топологии</p> <p>14. В текущее время по сети может проходить только одно сообщение при топологии</p> <p>15. Сообщения «идут» во всех направлениях при топологии</p> <p>....</p> <p>Примерные тесты по разделу Информатика и информационные технологии.pdf</p>
Промежуточный: зачет	<p>Обязательное выполнение практических заданий по темам:</p> <ol style="list-style-type: none"> 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 <p>Дополнительные задания</p> <ol style="list-style-type: none"> 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 балльно-рейтинговой оценки.pdf

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

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

из них: учебно-методическое обеспечение самостоятельной работы студента:

6. Классификация программного обеспечения
7. Архиваторы
8. Компьютерные вирусы и антивирусная защита
9. Базовые технологии компьютерных сетей
10. Обмен информацией в глобальных и локальных сетях

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Проблемы профилактики и противодействия компьютерной преступности [Электронный ресурс] : аннотир. рек. библиогр. указ. 2001-2011 / сост.: О. П. Шрейн, Е. А. Штумпф ; под ред. О. И. Ткаченко ; Юж.-Урал. гос. ун-т, Каф. Информационная безопасность ; Науч. б-ка ; ЮУрГУ	Электронный каталог ЮУрГУ	Интернет / Авторизованный
2	Дополнительная литература	Галатенко, В. А. Основы информационной безопасности : Курс лекций: Учеб. пособие	Электронный каталог ЮУрГУ	Интернет / Авторизованный

		для вузов по специальностям в обл. информ. технологий / В. А. Галатенко; Под ред. В. Б. Бетелина; Интернет-ун-т информ. технологий. М. : Интернет-Университет Информационных Технологий , 2006. 205 с.		
3	Дополнительная литература	Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие / В. П. Мельников и др.; под ред. С. А. Клейменова. - М. : Академия, 2009. 330, [1] с.	Электронный каталог ЮУрГУ	Интернет / Авторизованный
4	Основная литература	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)	Гарант	Интернет / Свободный
5	Основная литература	Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"	Гарант	Интернет / Свободный
6	Основная литература	Постановление Правительства РФ от 31 июля 2014 г. N 758 "О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей"	Гарант	Интернет / Свободный
7	Основная литература	Федеральный закон от 23 июня 2016 г. N 208-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и Кодекс Российской Федерации об административных правонарушениях"	Гарант	Интернет / Свободный
8	Основная литература	Федеральный закон от 28 декабря 2010 г. N 390-ФЗ "О безопасности"	Гарант	Интернет / Свободный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

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

Перечень используемых информационных справочных систем:

1. -Консультант Плюс(31.07.2017)
2. -Гарант(31.12.2018)

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)	Компьютер (рабочее место пользователя) - 16 шт. (Системный блок Intel 10 series/c 230/Celeron G3930 2.9GHz/4Gb/500Gb, монитор Samsung 943 LCD 19", клавиатура, мышь); системное программное обеспечение Windows 7 pro (тип лицензии: DreamSpark Retail Key), прикладное программное обеспечение Офисный пакет Microsoft 2007 (тип лицензии: Подписка MSDN (44938187))
Самостоятельная работа студента	112 (8Э)	Компьютер (рабочее место пользователя) - 16 шт. (Системный блок Intel 10 series/c 230/Celeron G3930 2.9GHz/4Gb/500Gb, монитор Samsung 943 LCD 19", клавиатура, мышь); системное программное обеспечение Windows 7 pro (тип лицензии: DreamSpark Retail Key), прикладное программное обеспечение Офисный пакет Microsoft 2007 (тип лицензии: Подписка MSDN (44938187))