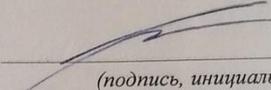


МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ
Декан факультета
юридического

(наименование ф-та полностью)

 С.В. Шевелева

(подпись, инициалы, фамилия)

« 22 » февраля 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

(наименование дисциплины)

Направление подготовки (специальность)

40.05.02

(шифр согласно ФГОС)

Правоохранительная деятельность

и наименование направления подготовки (специальности)

Обеспечение безопасности в уголовно-исполнительной системе

наименование профиля, специализации или магистерской программы

Форма обучения

заочная

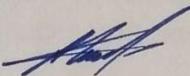
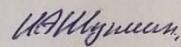
(очная, очно-заочная, заочная)

Курск - 2017 г.

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования специальности 40.05.02 Правоохранительная деятельность и на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол №5 от 30 января 2017 года.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения студентов по специальности 40.05.02 Правоохранительная деятельность на заседании кафедры уголовного права протокол №9 «13» 02 2017 года.

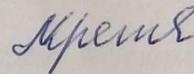
Зав. кафедрой уголовного права
Разработчик программы:
к.т.н., доцент

Байбарин А.А.

Шуклин И.А.

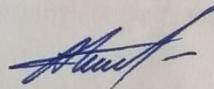
/Директор научной библиотеки



Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № 4 «29» декабря 2016 г. на заседании кафедры уголовного права «1» 09 2017 г. протокол № 1

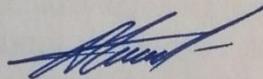
Зав. кафедрой



Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № 9 «26» 03 2018 г. на заседании кафедры уголовного права «31» 08 2018 г. протокол № 1.

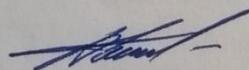
Зав. кафедрой



Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № 9 «26» 03 2018 г. на заседании кафедры уголовного права «28» 06 2019 г. протокол № 14.

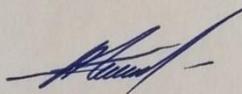
Зав. кафедрой



Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № 7 «29» 03 2019 г. на заседании кафедры уголовного права «25» 06 2020 г. протокол № 13.

Зав. кафедрой



Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № ___ «___» _____ 20__ г. на заседании кафедры уголовного права «___» _____ 20__ г. протокол № ___.

Зав. кафедрой

Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № ___ «___» _____ 20__ г. на заседании кафедры уголовного права «___» _____ 20__ г. протокол № ___.

Зав. кафедрой

Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № ___ «___» _____ 20__ г. на заседании кафедры уголовного права «___» _____ 20__ г. протокол № ___.

Зав. кафедрой

Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № ___ «___» _____ 20__ г. на заседании кафедры уголовного права «___» _____ 20__ г. протокол № ___.

Зав. кафедрой

Байбарин А.А.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 40.05.02 Правоохранительная деятельность, одобренного Ученым советом университета протокол № ___ «___» _____ 20__ г. на заседании кафедры уголовного права «___» _____ 20__ г. протокол № ___.

Зав. кафедрой

Байбарин А.А.

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1 Цель дисциплины

Формирование у студентов целостной системы базовых теоретических знаний основ информационной безопасности и практических умений использования современных методов обработки, преобразования и защиты информации в современных компьютерных системах, а также овладения студентами соответствующими общекультурными и профессиональными компетенциями в объеме осваиваемых видов и задач профессиональной деятельности, предусмотренных требованиями ФГОС ВО.

1.2 Задачи дисциплины

Основными задачами изучения дисциплины являются:

- приобретение обучающимися необходимых познаний в сфере информационной безопасности в контексте решения профессиональных задач по профилю юридической деятельности;
- формирование у обучающихся способностей соблюдения в профессиональной деятельности требований нормативных правовых актов в области информационной безопасности;
- получение обучающимися навыков в применении основных методов, способов и средств получения, хранения, поиска, систематизации, обработки, передачи и защиты информации при решении профессиональных задач в объеме предусмотренных ФГОС ВО видов профессиональной деятельности;
- развитие способностей обучающихся в работе с различными информационными ресурсами и применении современных способов борьбы с несанкционированным блокированием, доступом, копированием, изменением и сбором информации.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Обучающиеся должны знать:

- основные закономерности создания и функционирования информационных процессов в правовой сфере;
- основы государственной политики в области информатики;
- методы и средства поиска, систематизации и обработки правовой информации;
- практические способы построения систем защиты информации;
- положения Концепции информационной безопасности России в части угроз и опасностей, стратегии и тактики, внешних и внутренних факторов, влияющих на состояние национальной безопасности;

уметь:

- применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа правовой и служебной информации;

- оперировать информационными понятиями и категориями;
- строить системы защиты информации;
- осуществлять формирование режима информационной безопасности;
- определять необходимую степень защиты;

владеть:

- навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности;

- навыками обеспечения режима информационной безопасности в организации;

- навыками организации достоверной, безопасной передачи информации в компьютерных и других информационных системах связи.

У обучающихся формируется следующие компетенции:

- способность выпускника соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-22).

2 Указание места дисциплины в структуре образовательной программы

«Основы информационной безопасности» представляет дисциплину по выбору с индексом Б1.В.ДВ.4.1 базовой части учебного плана подготовки 40.05.02 Правоохранительная деятельность, изучаемую на 2 курсе в 3 семестре.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единиц (з.е.), 108 часов.

Таблица 3 – Объём дисциплины

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	8,1
в том числе:	
лекции	2
лабораторные занятия	-
практические занятия	6
экзамен	не предусмотрен
зачет	0,1
курсовая работа (проект)	не предусмотрена
расчётно-графическая (контрольная) работа	не предусмотрена

Аудиторная работа (всего):	8
в том числе:	
лекции	2
лабораторные занятия	-
практические занятия	6
Самостоятельная работа обучающихся (всего)	95,9
Контроль/экс (подготовка к экзамену)	-

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	Введение в дисциплину «Основы информационной безопасности»	Цели, задачи, структура и содержание учебной дисциплины, формируемые компетенции и процедура проведения текущего контроля. Информационная безопасность и ее составные части. Понятия целостности, конфиденциальности, аутентичности и доступности информации. Защищенность информационных ресурсов, систем и технологий.
2	Сущность проблемы информационной безопасности (ИБ)	Актуальность и важность проблемы обеспечения ИБ. Предпосылки, направления и перспективы киберпреступности. Основные понятия в области информационной безопасности. Аспекты ИБ: доступность, целостность, конфиденциальность.
3	Основные угрозы информационной безопасности	Понятие угрозы ИБ. Характеристики информационного ресурса как объекта защиты. Классификация и характеристика угроз ИБ. Угрозы случайные и преднамеренные, внешние и внутренние, стихийного и искусственного характера. Проявления, последствия и основные способы реализации угроз.
4	Правовое обеспечение информационной безопасности	Понятие правового обеспечения ИБ. Особенности информации как объекта права. Государственная политика РФ в области правового обеспечения. Уровни правового регулирования в сфере ИБ. Основные конституционные и правовые нормы в области ИБ. Понятия банковской, коммерческой и служебной тайны. Наказания за преступления в сфере компьютерной информации. Зарубежное законодательство в области ИБ.
5	Организационное обеспечение информационной безопасности	Понятие организационного обеспечения ИБ. Характеристика организационных методов обеспечения ИБ. Структура государственных органов РФ, осуществляющих правотворчество и правоприменение в области ИБ. Организационно - распорядительные документы, связанные с защитой сведений конфиденциального характера. Концепция построения комплексной системы обеспечения ИБ и защиты информации.
6	Защита информации в компьютерных системах от случайных угроз и традиционного	Организация дублирования информации. Повышение надежности и отказоустойчивости компьютерных систем. Блокировка ошибочных операций и оптимизация взаимодействия пользователей с компьютерной системой.

	шпионажа	Минимизация ущерба от аварий и стихийных бедствий. Защита конфиденциальных информационных ресурсов, противодействие наблюдению в оптическом диапазоне и прослушиванию. Методы и средства защиты от электромагнитных излучений и наводок
7	Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах	Защита информации в компьютерных системах от несанкционированного доступа. Методы и средства защиты от несанкционированного изменения структур компьютерных систем. Криптографические методы защиты информации. Криптология, криптография и криптоанализ. Классификация криптографических методов. Симметричное и асимметричное шифрование. Электронная подпись.
8	Защита информации в распределенных компьютерных системах	Особенности защиты информации в распределенных компьютерных системах. Характеристика угроз ИБ в распределенных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Подтверждение подлинности информации и взаимодействующих процессов. Практические рекомендации пользователям глобальной сети Интернет по обеспечению информационной безопасности.
9	Защита компьютерных систем от вирусов и вредоносных программ	Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения

Таблица 4.1.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел учебной дисциплины	Виды учебной деятельности (в часах)		Учебно-методические материалы	Формы текущего контроля успеваемости и (по неделям семестра)	Компетенции
		лек. час	№ пр.			
1	Введение в дисциплину «Основы информационной безопасности»	2	1	У-1, У-10, У-11, У-12	КО, МК 24-25 нед.	ПК-22
2	Сущность проблемы информационной безопасности (ИБ)	2	2	У-1, У-10, У-11, У-12	КО, МК 26-27 нед.	ПК-22
3	Основные угрозы информационной безопасности	2	3	У-1, У-10, У-11, У-12	КО, МК 28-29 нед.	ПК-22
4	Правовое обеспечение информационной безопасности		4	У-1, У-10, У-11, У-12, МУ-1	КО, МК 30-31 нед.	ПК-22
5	Организационное обеспечение информационной безопасности	2	5	У-1, У-3, У-10, У-11, У-12, МУ-1	С, КО, МК 32-33 нед.	ПК-22
6	Защита информации в	2	6	У-2, У-3, У-5	С, КО, МК	ПК-22

	компьютерных системах от случайных угроз и традиционного шпионажа			У-6, У-7, У-8, У-12, МУ-1	34-35нед.	
7	Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах	2	7	У-2, У-3, У-5, У-6, У-7, У-8, У-9, МУ-1	С, КО, МК 36-37нед.	ПК-22
8	Защита информации в распределенных компьютерных системах	2	8	У-2, У-3, У-5, У-6, У-7, У-8, У-9, МУ-1	С, КО, МК 38-39нед.	ПК-22
9	Защита компьютерных систем от вирусов и вредоносных программ	2	9	У-2, У-3, У-5, У-6, У-7, У-8, У-9, МУ-1	С, КО, МК 40-41 нед.	ПК-22

С – собеседование, КО – контрольный опрос, МК – машинный контроль.

4.2 Лабораторные работы и (или) практические занятия

Таблица 4.2.1 – Практические занятия

№ п/п	Наименование практического (семинарского) занятия	Объем, час.
1.	Поиск и систематизация информации на тему «Информационная безопасность и ее составные части». Разработка текстового документа и его презентация	4
2.	Поиск и систематизация информации на тему «Актуальность и важность проблемы обеспечения информационной безопасности». Разработка текстового документа и его презентация	4
3.	Поиск и систематизация информации на тему «Основные угрозы информационной безопасности». Разработка текстового документа и его презентация	4
4.	Поиск и систематизация информации на тему «Правовое обеспечение информационной безопасности». Разработка текстового документа и его презентация	4
5.	Поиск и систематизация информации на тему «Организационное обеспечение информационной безопасности». Разработка текстового документа и его презентация	4
6.	Поиск и систематизация информации на тему «Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа». Разработка текстового документа и его презентация	4
7.	Поиск и систематизация информации на тему «Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах». Разработка текстового документа и его презентация	4
8.	Поиск и систематизация информации на тему «Защита информации в распределенных компьютерных системах». Разработка текстового документа и его презентация	4
9.	Поиск и систематизация информации на тему «Защита компьютерных систем от вирусов и вредоносных программ». Разработка текстового документа и его презентация	4
	Итого:	36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время на выполнение СРС, час.
1	Информационная безопасность и ее составные части	24-я неделя	6
2	Актуальность и важность проблемы обеспечения Информационная безопасность	26-я неделя	6
3	Основные угрозы информационной безопасности	28-я неделя	6
4	Правовое обеспечение информационной безопасности	30-я неделя	6
5	Организационное обеспечение информационной безопасности	32-я неделя	6
6	Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа	34-я неделя	6
7	Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах	36-я неделя	6
8	Защита информации в распределенных компьютерных системах	38-я неделя	6
9	Защита компьютерных систем от вирусов и вредоносных программ	40-я неделя	6
	Итого		54

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

- путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;
- заданий для самостоятельной работы;
- банка тестов, кейс-задач;
- методических указаний к выполнению практических занятий и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 о направлении подготовки (специальности) 40.05.02 Правоохранительная деятельность реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках курса предусмотрены встречи с ведущими экспертами и специалистами СПС КонсультантПлюс, Гарант и правоохранительных органов.

Удельный вес занятий, проводимых в интерактивных формах, составляет 33% аудиторных занятий: 6 часов – лекции, 12 часов – практические занятия, согласно УП.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	Лекция №2. Сущность современных проблем информационной безопасности	Мультимедийные технологии визуализации учебной информации	1,5
2	Практическое занятие №2. Поиск и систематизация информации на тему «Актуальность и важность проблемы обеспечения информационной безопасности»	Компьютерный класс. Пакет программ MicrosoftOffice. СПС КонсультантПлюс, Гарант. Интернет. Разбор конкретных ситуаций	3
3	Лекция №3. Основные угрозы информационной безопасности	Мультимедийные технологии визуализации учебной информации	1,5
4	Практическое занятие №3. Поиск и систематизация информации на тему «Основные угрозы информационной безопасности»	Компьютерный класс. Пакет программ MicrosoftOffice. СПС КонсультантПлюс, Гарант. Интернет. Разбор конкретных ситуаций	2
5	Лекция №4. Правовое обеспечение информационной безопасности	Мультимедийные технологии визуализации учебной информации	1,5
6	Практическое занятие №4. Поиск и систематизация информации на тему	Компьютерный класс. Пакет программ MicrosoftOffice. СПС КонсультантПлюс,	3

	«Правовое обеспечение информационной безопасности»	Гарант. Интернет. Разбор конкретных ситуаций	
7	Лекция №5. Организационное обеспечение информационной безопасности	Мультимедийные технологии визуализации учебной информации	1,5
8	Практическое занятие №5. Поиск и систематизация информации на тему «Организационное обеспечение информационной безопасности»	Компьютерный класс. Пакет программ MicrosoftOffice. СПС КонсультантПлюс, Гарант. Интернет. Разбор конкретных ситуаций	3
Итого			18

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенции

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
ПК-22 – способность выпускника соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности		Основы информационной безопасности	Делопроизводство и режим секретности

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели, критерии и шкала оценивания уровней сформированности компетенций (частей компетенций)

Код компетенции/ этап (указывается название этапа из п. 7.1)	Показатели оценивания компетенций	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
ПК-22/ начальный, основной	1. Доля освоенных обучающимися знаний, умений, навыков от общего объема ЗУН, установлен	Знать: нормативные правовые акты в области защиты информации и противодействия техническим разведкам; основные методы, способы и мероприятия по обеспечению	Знать: нормативные правовые акты в области защиты информации и противодействия техническим разведкам; основные методы, способы и мероприятия по обеспечению	Знать: нормативные правовые акты в области защиты информации и противодействия техническим разведкам; основные методы, способы и мероприятия по обеспечению

<p>ных в п. 1. ЗРПД</p> <p>2. Качество освоенных обучающи мся знаний, умений, навыков</p> <p>3. Умение применять знания, умения, навыки в типовых и нестандар тных ситуациях</p>	<p>информационной безопасности в профессиональной деятельности, предусматривающие деятельность по воспроизведению. Уметь: использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированног о доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации в ситуациях с внешне заданным алгоритмическим описанием (подсказкой). Владеть: способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности при решении профессиональных задач с внешне заданным алгоритмическим описанием (подсказкой)</p>	<p>информационной безопасности в профессиональной деятельности, предполагающие применение в ситуациях, аналогичным обучающим. Уметь: использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированно го доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации в ситуациях, аналогичным обучающим или ранее встречавшихся в практике. Владеть: способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности при решении профессиональных задач в ситуациях, аналогичным обучающим</p>	<p>информационной безопасности в профессиональной деятельности, использующиеся для решения задач, требующих установления новых связей между понятиями. Уметь: использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированног о доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации в нестандартных ситуациях, требующих установления новых связей между понятиями, явлениями и процессами. Владеть: способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности при решении профессиональных задач, требующих</p>
--	---	---	---

				установления новых связей между понятиями, явлениями и процессами
--	--	--	--	---

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	Введение в дисциплину «Основы информационной безопасности»	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий	В объёме ПЗ №1	Согласно табл.7.2
2	Сущность проблемы информационной безопасности (ИБ)	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий	В объёме ПЗ №2	Согласно табл.7.2
3	Основные угрозы информационной безопасности	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий	В объёме ПЗ №3	Согласно табл.7.2
4	Правовое обеспечение информационной безопасности	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий	В объёме ПЗ №4	Согласно табл.7.2
5	Организационное обеспечение информационной безопасности	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий, кейс-задач	В объёме ПЗ №5	Согласно табл.7.2
6	Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий, кейс-задач	В объёме ПЗ №6	Согласно табл.7.2
7	Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий, кейс-задач	В объёме ПЗ №7	Согласно табл.7.2
8	Защита информации в распределенных	ПК-22	Лекция, практическое	Тест, решение разноуровневых	В объёме	Согласно

	компьютерных системах		занятие, СРС	задач и заданий, кейс-задач	ПЗ №8	табл.7.2
9	Защита компьютерных систем от вирусов и вредоносных программ	ПК-22	Лекция, практическое занятие, СРС	Тест, решение разноуровневых задач и заданий, кейс-задач	В объёме ПЗ №9	Согласно табл.7.2

Примеры типовых контрольных заданий для текущего контроля

Тест по теме №1 включает вопросы и задания с выборочными ответами. Типовыми являются следующие:

1. *Состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства называют ...* 1. информационной безопасностью; 2. защитой интересов государства в информационной сфере; 3. защитой интересов общества в информационной сфере; 4. защитой интересов личности в информационной сфере; 5. защитой информации.

2. *Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации, это ...* 1. источник угрозы безопасности информации; 2. фактор, воздействующий на защищаемую информацию; 3. уязвимость информационной системы; 4. несанкционированное воздействие на информацию; 5. угроза безопасности информации.

3. *Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты, это ...* 1. объект защиты информации; 2. защищаемая информация; 3. носитель защищаемой информации; 4. защищаемый объект информатизации; 5. защищаемая информационная система.

4. *Порядок и правила применения определенных принципов и средств защиты информации это ...* 1. способ защиты информации; 2. защита информации от утечки; 3. защита информации от несанкционированного воздействия; 4. защита информации от непреднамеренного воздействия; 5. защита информации от несанкционированного доступа.

5. *Политика безопасности и комплекс процедур по безопасности информационной среды формируется на ...* 1. законодательном уровне; 2. административном уровне; 3. программно-техническом уровне; 4. пользовательском уровне; 5. на всех перечисленных уровнях.

Вопросы собеседования по теме 3 «Основные угрозы информационной безопасности».

1. Понятие угрозы информационной безопасности.
2. Характеристики информационного ресурса как объекта защиты.
3. Классификация и характеристика угроз информационной безопасности.
4. Угрозы случайные и преднамеренные, внешние и внутренние, стихийного и искусственного характера.

5. Проявления, последствия и основные способы реализации угроз.

Разноуровневые задачи

Задача №1 (репродуктивный уровень). Выполнить поиск в справочной правовой системе документ, определяющий четыре основные составляющие национальных интересов Российской Федерации в информационной сфере и сохранить эту информацию в текстовом редакторе.

Задача №2 (реконструктивный уровень). Найти в справочной правовой системе информацию, характеризующую угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России и разработать презентацию данных угроз.

Задача №3 (творческий уровень). Используя возможности СПС Консультант Плюс или Гарант найти и сохранить в текстовый документ информацию о результатах исследования возможностей защиты персональных данных в прикладных интеллектуальных системах от девяти видов технической компьютерной разведки по актуальным требованиям российского законодательства.

Кейс-задачи

Кейс-задача №1. «Законодательство о защите информации»

Ситуация. Руководитель потребовал подготовить презентацию требований нормативных правовых актов по вопросам информационной безопасности.

Используя возможности СПС КонсультантПлюс или Гарант найти необходимые документы, сохранить их список и подготовить презентацию основных требований в области информационной безопасности.

Кейс-задача №2. «Создание подборки документов для реферата на заданную тему»

Ситуация. Преподаватель дал задание подготовить подборку документов для разработки реферата на тему «Кибертерроризм».

Создать папку «Кибертерроризм» и используя возможности СПС КонсультантПлюс или Гарант найти и сохранить в папку все материалы в соответствии с темой задания: а) основные акты федеральных и региональных органов власти; б) подборку судебных решений высших судебных инстанций, Конституционного суда, ФАС округов; в) подборку статей научных журналов по юриспруденции.

Кейс-задача №3. «Выполнение исследовательских практических заданий»

Ситуация. Руководитель дал задание подготовить информацию об изменении нормативных правовых актов по следующим вопросам: 1). Законодательство о персональных данных; 2). Законодательство в области интеллектуальной собственности; 3). Законодательство о коммерческой тайне; 4). Законодательство о государственной тайне; 5). Законодательство об электронной цифровой подписи.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме тестирования (бланкового и/или компьютерного).

Для тестирования используются контрольно-измерительные материалы (КИМ) – задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для промежуточной аттестации

1. Назовите государственные органы РФ, составляющие организационную основу системы обеспечения информационной безопасности.

2. Раскройте сущность защиты информации в компьютерных системах от несанкционированного доступа.

3. Дайте характеристику методов и средств защиты от несанкционированного изменения структур компьютерных систем.

4. Раскройте сущность особенностей защиты информации в распределенных компьютерных системах.

5. Назовите меры профилактики заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Стандарт университета СТУ 04.02.035-2007 «Учебно-методический комплекс дисциплины. Требования к структуре, содержанию, оформлению, порядку разработки и управлению»;

- Инструкция И 02.018-2015 «Инструкция по заполнению фонда оценочных средств»;

- Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

- Положение П 02.034-2014 «О проведении текущего контроля успеваемости и промежуточной аттестации студентов в ЮЗГУ»;

- Методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4– Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Практическое занятие №1. Поиск и систематизация информации на тему «ИБ и ее составные части». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	4	Выполнил, доля правильных ответов более 50%
Практическое занятие №2. Поиск и систематизация информации на тему «Актуальность и важность проблемы обеспечения ИБ». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	4	Выполнил, доля правильных ответов более 50%
Практическое занятие №3. Поиск и систематизация информации на тему «Основные угрозы информационной безопасности». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	4	Выполнил, доля правильных ответов более 50%
Практическое занятие №4. Поиск и систематизация информации на тему «Правовое обеспечение информационной безопасности». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил, доля правильных ответов более 50%
Практическое занятие №5. Поиск и систематизация информации на тему «Организационное обеспечение информационной безопасности». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил, доля правильных ответов более 50%
Практическое занятие №6. Поиск и систематизация информации на тему «Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил, доля правильных ответов более 50%
Практическое занятие №7. Поиск и систематизация информации на тему «Методы и средства защиты информации от	3	Выполнил, доля правильных ответов менее	6	Выполнил, доля правильных ответов более

несанкционированного доступа и изменения структур в компьютерных системах». Разработка текстового документа и его		50%		50%
Практическое занятие №8. Поиск и систематизация информации на тему «Защита информации в распределенных компьютерных системах». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил, доля правильных ответов более 50%
Практическое занятие №9. Поиск и систематизация информации на тему «Защита компьютерных систем от вирусов и вредоносных программ». Разработка текстового документа и его презентация	3	Выполнил, доля правильных ответов менее 50%	6	Выполнил, доля правильных ответов более 50%
Итого успеваемость	24		48	
Посещаемость			16	
Зачёт			36	
Итого:	24		100	

Для промежуточной аттестации, проводимой в форме тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ – 16заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная учебная литература

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.
2. Калущкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калущкий, А.Г. Спеваков ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2014. – 179 с.
3. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Елена Анатольевна Богданова [и др.]. - М. : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.
4. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2012. – 616 с.

8.2. Дополнительная учебная литература

5. Богомолова, О. Б. Защита компьютера от вредоносных воздействий [Электронный ресурс]: практикум / О. Б. Богомолова, Д. Ю. Усенков. – М.: БИНОМ. Лаборатория знаний, 2012. – 179 с. // Режим доступа – <http://biblioclub.ru/index.php?page=book&id=221695&sr=1>
6. Защита данных геоинформационных систем [Текст] / Людмила Климентьевна Бабенко [и др.]. - М. : Гелиос АРВ, 2010. - 336 с. : ил.
7. Ищейнов, В. Я. Защита конфиденциальной информации [Текст] : учебное пособие / Вячеслав Яковлевич Ищейнов, Михаил Владимирович Мецатунян. - М. : Форум, 2013. - 256 с.
8. Носенко, В. А. Защита интеллектуальной собственности [Текст] : учебное пособие / Владимир Андреевич Носенко, Анна Вадимовна Степанова. - Старый Оскол : ТНТ, 2013. - 192 с.
9. Перетолчин, А.С. Защита Windows от сбоев [Электронный ресурс]: практикум / А.С. Перетолчин. – Новосибирск: Сибирское университетское издательство, 2008. – 112 с. // Режим доступа – <http://biblioclub.ru/index.php?page=book&id=57378&sr=1>
10. Сергеева, Ю.С. Защита информации. Конспект лекций [Электронный ресурс]: учебное пособие / Ю.С. Сергеева. – М.: А-Приор, 2011. – 128 с. // Универ. библио. online – <http://biblioclub.ru/index.php?page=book&id=72670&sr=1>
11. Сычев, Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-практическое пособие / Ю.Н. Сычев. – М.: Евразийский открытый институт, 2010. – 328 с. // Режим доступа – <http://biblioclub.ru/index.php?page=book&id=90790&sr=1>
12. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: курс лекций. – М.: Интернет-Университет Информационных Технологий, 2011. – 138 с. // Режим доступа – <http://biblioclub.ru/index.php?page=book&id=233763&sr=1>

8.3 Перечень методических указаний

1. **Организационно-правовые механизмы обеспечения информационной безопасности** [Электронный ресурс]: методические указания по подготовке к практическим занятиям для студентов всех форм обучения специальности 030900.68 «Юриспруденция» / Юго-Западный государственный университет ; сост. А. А. Гребеньков [и др.]. - Электрон.текстовые дан. (534 КБ). - Курск : ЮЗГУ, 2014. - 30 с. : прил.

8.4 Другие учебно-методические материалы

1. **ГОСТ Р ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий** [Текст] . Ч. 2 : Функциональные требования безопасности. - Введ. 2009.10.01 ; взамен ГОСТ Р ИСО/МЭК 15408-2-2002. – М. :Стандартинформ, 2009. – 167 с. – (Национальный стандарт РФ).

2. ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Информационная технология [Текст] . Ч. 3 : Требования доверия к безопасности. - Введ. 2009.10.01 ; взамен ГОСТ Р ИСО/МЭК 15408-3-2002. – М. :Стандартинформ, 2009. – 112 с. – (Национальный стандарт РФ).

3. Стохастические методы и средства защиты информации в компьютерных системах и сетях [Текст] / М. А. Иванов [и др.] ; под ред. И. Ю. Жукова. - М. : КУДИЦ-ПРЕСС, 2009. - 512 с. - ISBN 978-5-91136-068-9 : 811р. 36к. Кол-во экземпляров: всего – 1

4. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. <http://www.kremlin.ru>. Сайт Президента России: [Электронный ресурс].

2. <http://www.government.ru>. Сайт Правительства Российской Федерации: [Электронный ресурс].

3. <http://www.council.gov.ru>. Сайт Совета Федерации: [Электронный ресурс].

4. <http://www.duma.gov.ru>. Сайт Государственной Думы: [Электронный ресурс].

5. <http://pravo.fso.gov.ru/> Официальный интернет-портал правовой информации. Государственная система правовой информации. [Электронный ресурс].

6. <http://crimestat.ru/> Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации. [Электронный ресурс].

7. <http://www.znanium.com/bookread.php?book=405000> Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.

8. <http://www.znanium.com/bookread.php?book=335362> Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - Режим доступа:

9. <http://www.knigafund.ru/books/172320> Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. [Электронный ресурс]: Автор: Куняев Н.Н. Издательство: Логос, 2010 г. 346 с.

10. <https://biblioclub.ru/> - ЭБС «Университетская библиотека онлайн»

11. lib.swsu.ru/ - Электронная библиотека ЮЗГУ

12. <https://e.lanbook.com/> - ЭБС «Лань»

10 Методические указания для обучающихся по освоению дисциплины

Содержание дисциплины изучается на лекциях и практических занятиях, порядок проведения которых излагается в соответствующих планах и методических указаниях, а также в процессе самостоятельной работы обучаемых в объеме

отведенного времени для подготовки к выполнению заданий практических занятий и промежуточному контролю.

Лекции проводятся для потоков в лекционной аудитории с использованием мультимедийных технологий визуализации учебной информации. На лекциях преподаватель излагает и разъясняет основные понятия темы, связанные с ней теоретические и практические проблемы, дает рекомендации для самостоятельной работы при подготовке к практическим занятиям. В ходе лекции обучающиеся должны внимательно слушать и конспектировать лекционный материал, активно участвовать в обсуждении проблемных вопросов.

Практические занятия организуются по группам в компьютерном классе в активных и интерактивных формах в сочетании с внеаудиторной работой с целью исследования возможностей изучаемых информационных технологий и отработки практических умений в использовании изучаемых информационных технологий для формирования и развития профессиональных навыков и соответствующих компетенций обучающихся в решении профессиональных задач.

При выполнении заданий практических занятий обучающимся рекомендуется пользоваться справочным материалом программного обеспечения *ОС Windows* и *MicrosoftOffice* персонального компьютера, рекомендованной литературой и цифровыми образовательными ресурсами соответствующих методических материалов, размещенных в сети Интернета и локальной сети университета. Они включают текстовые теоретические и методические материалы, а также графические и видеоматериалы по изучаемым темам, в которых содержится изучаемый новый материал, описание и методические рекомендации по подготовке и проведению практических заданий в Web-формате, а также образцы документов и другие раздаточные материалы.

В качестве раздаточного материала обучающимся заблаговременно выдаются электронные версии методических указаний к практическим занятиям, которые они при необходимости размножают самостоятельно в нужном количестве на бумажном носителе или сохраняют на флэш-память.

Результаты выполнения заданий практического занятия разрешается сохранять на флэш-память студента для подготовки к зачёту и экзамену. Рабочие файлы в персональном компьютере компьютерного класса **УДАЛЯЮТСЯ!**

Обучающимся, не выполнившим в полном объеме все задания практического занятия, разрешается отработать их самостоятельно и представить результаты отработки в сроки, определенные преподавателем, с использованием личной флэш-памяти и демонстрацией отработанных материалов в компьютерном классе или предоставлением материалов по электронной почте.

Самостоятельная работа обучающихся состоит в проработке литературы и выполнении заданий в соответствии с рекомендациями преподавателя,

Подготовка к выполнению заданий обучающимися предусматривает: ознакомление с заданием на практическое занятие; выбор средств и составление процедур решения конкретных задач; формулирование проблемных вопросов для обсуждения в начале занятия.

Для эффективной реализации целей практических занятий обучающимся рекомендуется регулярно обновлять навыки работы с информационными технологиями: с операционной системой ОС Windows и программным обеспечением персонального компьютера ПО MicrosoftOffice; с локальной вычислительной сетью (ЛВС) университета и глобальной сетью Интернет; с локальными версиями СПС Консультант Плюс, Гарант; с тренинго-тестирующими системами (ТТС) СПС Консультант Плюс, Гарант; с другими информационными технологиями.

Обучающиеся осуществляют самоконтроль результатов самостоятельной работы по тем же критериям и показателям, которые определяются преподавателем для проведения внешнего контроля. Это позволяет студенту объективно оценить не только результаты обучения, но и уровень сформированности соответствующих компетенций и развития личностных психологических качеств, важных для профессиональной деятельности будущего юриста.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

При проведении аудиторных занятий используются следующие информационные технологии: - сетевая версия СПС КонсультантПлюс, сетевая версия СПС Гарант, пакет программ MicrosoftOffice, сеть интернета и др.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционная аудитория; компьютерные классы университета (20-23 ПК) ОС WindowsXP; программное обеспечение MicrosoftOffice; мультимедийная установка (проекционно-компьютерная система); экран для проекционно-компьютерной системы; телевизионная плазменная панель; вычислительная сеть университета с локальными версиями СПС Консультант Плюс, Гарант; сеть Интернета.

13 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			
1	-	4, 9	-	-	2	01.09.17	Протокол заседания кафедры №1 от 01.09.17 г.

Приложение к рабочей программе дисциплины

В качестве результатов освоения дисциплины может быть зачтен онлайн-курс «**Основы водоснабжения и водоотведения**», разработанный ФГБОУ ВО «Юго-Западный государственный университет», расположенный на портале «Современная цифровая образовательная среда Российской Федерации» (<https://online.edu.ru>).

Прямая ссылка на онлайн-курс - <https://online.edu.ru/public/course?faces-redirect=true&cid=11235368>