Программа
учебной дисциплины

ОП.17.
ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2020 г.

РАССМОТРЕНА
на заседании ЦМК
уголовно-правовых
дисциплин
протокол № 4
от «23» мая 2020 г.
Председатель ЦМК
_____ П.В. Пошелов

УТВЕРЖДЕНА
Директор колледжа
_____ Ю.А. Бурдельная
«23» мая 2020 г.

Программа учебной дисциплины «Правовые основы информационной безопасности» разработана на основе Федеральных государственных образовательных стандартов (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 40.02.02 Правоохранительная деятельность.

Организация-разработчик: частное профессиональное образовательное учреждение «Омский юридический колледж»

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Область применения программы

Программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 40.02.02 Правоохранительная деятельность.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы.

Дисциплина входит в профессиональный цикл (общепрофессиональные дисциплины) и введена за счет часов вариативной части образовательной программы.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины студент должен освоить знания и умения, необходимые для формирования общих и профессиональных компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 3. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 7. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 12. Выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета.

ОК 14. Организовывать свою жизнь в соответствии с социально значимыми представлениями о здоровом образе жизни, поддерживать должный уровень физической подготовленности, необходимый для социальной и профессиональной деятельности.

ПК 1.1. Юридически квалифицировать факты, события и обстоятельства. Принимать решения и совершать юридические действия в точном соответствии с законом.

ПК 1.2. Обеспечивать соблюдение законодательства субъектами права.

ПК 1.3. Осуществлять реализацию норм материального и процессуального права.

ПК 1.4. Обеспечивать законность и правопорядок, безопасность личности, общества и государства, охранять общественный порядок.

ПК 1.5. Осуществлять оперативно-служебные мероприятия в соответствии с профилем подготовки.

ПК 1.6. Применять меры административного пресечения правонарушений, включая применение физической силы и специальных средств.

ПК 1.7. Обеспечивать выявление, раскрытие и расследование преступлений и иных правонарушений в соответствии с профилем подготовки.

ПК 1.11. Обеспечивать защиту сведений, составляющих государственную тайну, сведений конфиденциального характера и иных охраняемых законом тайн.

ПК 2.2. Осуществлять документационное обеспечение управленческой деятельности.

ПК 1.13. Осуществлять свою профессиональную деятельность во взаимодействии с сотрудниками правоохранительных органов, органов местного самоуправления, с представителями общественных объединений, с муниципальными органами охраны общественного порядка, трудовыми коллективами, гражданами.

В результате освоения учебной дисциплины обучающийся должен:

уметь:

- применять действующую законодательную базу в области информационной безопасности;
- анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития;
- организовывать работу с персоналом, обладающим конфиденциальной информацией;
- организовывать работу по обеспечению технической защиты информации с ограниченным доступом (конфиденциальной информации) на территории РФ.

знать:

– основные направления построения информационного общества в Российской Федерации;

– основные признаки, понятия и цели обеспечения информационной безопасности;

- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

1.4. Активные и интерактивные образовательные технологии, используемые на занятиях

Групповые дискуссии, решение ситуационных задач, метод «круглого стола», семинары, мультимедийные презентации, деловые и ролевые игры, кейс-метод.

1.5. Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины

Максимальная учебная нагрузка обучающегося 72 часов, в том числе:
обязательная аудиторная учебная нагрузка обучающегося 48 часов;
самостоятельная работа обучающегося 24 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ДЛЯ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ

2.1. Объем учебной дисциплины и виды учебной работы (очная форма обучения)

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	72
аудиторная учебная нагрузка (всего)	48

в том числе:	
лекционные занятия	12
практические занятия	34
Самостоятельная работа обучающегося (всего)	24
Промежуточная аттестация **в форме дифференцированного зачета**	

2.2. Тематический план и содержание учебной дисциплины «Правовые основы информационной безопасности» (очная форма обучения)

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	**2**	**3**	**4**
Тема 1. Информационное общество и информационная безопасность.	**Содержание учебного материала**	-	1
	Понятие, предпосылки и характерные черты информационного общества. Стратегия развития информационного общества в РФ. Цель, задачи и принципы развития информационного общества в РФ. Контрольные значения показателей развития информационного общества в РФ. Национальные интересы РФ в информационной сфере. Основные составляющие национальных интересов РФ в информационной сфере. Внутренние и внешние угрозы информационной безопасности РФ, их источники. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности РФ.	-	
	Практические занятия	**2**	2
	1. Составление схемы методов обеспечения информационной безопасности РФ.	2	
Тема 2. Законодательство РФ в области информационной безопасности.	**Содержание учебного материала**	-	1
	Основные этапы развития российского законодательства об информации, информатизации и защите информации. Конституция РФ, уголовное, административное, гражданское законодательство, федеральные законы и иные нормативные акты. Предмет правового обеспечения информационной безопасности. Правовое обеспечение безопасности информации в форме сведений и сообщений. Содержание и структура законодательства. Проблемы правового обеспечения и защиты информации в современной России. Перспективы развития законодательства в области информационной безопасности.	-	
	Практические занятия	**4**	2
	1. Анализ федеральных законов в области информационной безопасности.	2	
	2. Решение тестовых заданий.	2	
Тема 3.	**Содержание учебного материала**	**2**	1

Государственная система защиты информации.	Организация работ по защите информации. Структура и основные функции государственной системы защиты информации. Государственные органы управления в области информационной безопасности, их права и обязанности.	2	
	Практические занятия	**4**	2
	1. Решение ситуационных задач с использованием нормативных правовых актов.	2	
	2. Решение тестовых заданий.	2	
Тема 4. **Информация как объект правового регулирования.**	**Содержание учебного материала**	-	1
	Структура информационной сферы и характеристика её элементов. Понятие и виды информации. Основные признаки информации, принципиальные для правового регулирования отношений по поводу информации. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации. Информационная сфера и информационная среда. Информационная инфраструктура. Сегменты информационной инфраструктуры. Обладатель информации, его права и обязанности. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации. Ответственность в информационной сфере.	-	
	Практические занятия	**4**	2
	1**.** Решение ситуационных задач с использованием нормативных правовых актов.	2	
	2. Решение тестовых заданий.	2	
Тема 5. **Правовое регулирование отношений по защите государственной тайны.**	**Содержание учебного материала**	2	2
	Государственная тайна как особый вид защищаемой информации. Засекречивание и рассекречивание сведений, составляющих государственную тайну; порядок распоряжения. Ответственность за нарушение режима государственной тайны.		
	Практические занятия	2	
	1. Решение ситуационных задач с использованием нормативных правовых актов.		
Тема 6. **Правовые режимы защиты конфиденциальной информации.**	**Содержание учебного материала**	2	1
	Правовое обеспечение защиты коммерческой тайны, персональных данных, служебной тайны, профессиональной тайны (банковская тайна, тайна следствия и судопроизводства, врачебная тайна и др.), тайны личной и семейной жизни и других тайн. Основные требования, предъявляемые к организации защиты конфиденциальной информации.		

	Правовые аспекты защиты информации, циркулирующей в телефонных и других линиях и системах связи. Правовое регулирование отношений предприятия с другими предприятиями, организациями и гражданами по защите конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов защиты конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).		
	Практические занятия	**2**	2
	1. Решение ситуационных задач с применением нормативных правовых актов	2	
Тема 7. Защита прав на результаты интеллектуальной собственности.	**Содержание учебного материала**	-	1
	Законодательство РФ об интеллектуальной собственности. Понятие интеллектуальной собственности. Объекты интеллектуальной собственности. Объекты и субъекты авторских прав. Исключительные авторские права. Смежные права. Объекты смежных прав. Правовая охрана программ для ЭВМ и баз данных. Защита авторских и смежных прав. Основы патентных правоотношений. Объекты патентных прав. Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Защита прав патентообладателей и авторов. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности.	-	
	Практические занятия	**2**	2
	1. Решение ситуационных задач.	2	
Тема 8. Защита информации в компьютерных системах.	**Содержание учебного материала**	**2**	1
	Защита информации от потери и разрушения. Защита информации от несанкционированного доступа. Пути несанкционированного доступа. Организационные меры защиты информации. Защита информации от утечки по техническим каналам. Технические каналы утечки информации. Каналы утечки речевой информации. Утечка информации по проводным коммуникациям. Основные методы, используемые при создании систем защиты информации. Основные способы защиты информации в телефонных каналах. Программные средства защиты информации. Криптографическая защита информационных ресурсов. Электронная подпись. Обеспечение защиты	2	

	информации в компьютерных сетях. Угрозы безопасности сети. Службы безопасности сети. Механизмы безопасности. Организация защиты информации в корпоративной сети. Структура схемы безопасности. Этапы построения политики безопасности.		
	Практические занятия	**2**	2
	1. Составление схемы основных методов и приемов защиты от несанкционированного доступа.	2	
Тема 9. Преступления в сфере компьютерной информации.	**Содержание учебного материала**	**2**	1
	Понятие компьютерных преступлений и их классификация. Уголовно-правовая характеристика компьютерных преступлений. Типичные цели и мотивы совершения компьютерных преступлений. Способы совершения компьютерных преступлений. Компьютерные вирусы. Жизненный цикл компьютерного вируса. Классификация компьютерных вирусов. Основные каналы распространения вирусов и других вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ. Тенденции развития компьютерной преступности в России. Характеристика неправомерного доступа к компьютерной информации. Особенности субъектов преступления. Категории субъектов преступления. Классификация личностей преступников, совершающих неправомерный доступ к компьютерной информации. Виды хакеров. Новая и старая школы хакеров. Криминологическая характеристика мошенничеств, совершаемых с использованием сети Интернет. Усредненный «портрет» среднестатистического Интернет-мошенника. Выявление и расследование мошенничеств, совершаемых с использованием сети Интернет.	2	
	Практические занятия	**8**	2
	1. Особенности закладок и защита от воздействия закладок. Пакеты антивирусных программ.	2	
	2. Перехват вывода на экран, перехват ввода с клавиатуры. Перехват и обработка файловых операций.	2	
	3. Защита информации от копирования. Защита программ от дисассемблирования.	2	
	4. Защита программ в оперативной памяти. Приемы работы с защищенными программами.	2	
Тема 10.	**Содержание учебного материала**	**2**	2

Расследование преступлений в сфере компьютерной информации.	Понятие оперативно-розыскной деятельности и оперативно-розыскных мероприятий по законодательству РФ. Органы, уполномоченные на осуществление оперативно-розыскной деятельности. Система правовых актов, регулирующих проведение оперативно-розыскных мероприятий. Криминалистические аспекты проведения расследования компьютерных преступлений. Особенности расследования преступлений в области компьютерной информации: привлечение специалистов, специфические приемы работы с машинными носителями, выдвижение и проверка следственных версий. Экспертиза преступлений в сфере компьютерной информации. Объекты компьютерно-технической экспертизы. Виды компьютерно-технических экспертиз. Группы вопросов, выносимых на разрешение компьютерно-технической экспертизы. Исследование программного обеспечения. Вопросы, разрешаемые при исследовании программного обеспечения. Исследование баз данных. Вопросы, разрешаемые при исследовании баз данных. Исследование аппаратного обеспечения ЭВМ. Вопросы, разрешаемые при исследовании аппаратного обеспечения ЭВМ.	2	
	Практические занятия	**2**	2
	1. Решение ситуационных задач	2	
Самостоятельная работа обучающихся по учебному курсу: 1. Работа с нормативными актами: Окинавская хартия глобального информационного общества, Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ, Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ Решение задач, кейсов. Работа с конспектами и учебной литературой.		24	
Дифференцированный зачет		2	
Итого:		**72**	

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ДЛЯ ЗАОЧНОЙ ФОРМЫ ОБУЧЕНИЯ

3.1. Объем учебной дисциплины и виды учебной работы (заочная форма обучения)

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	72
аудиторная учебная нагрузка (всего)	12
в том числе:	
лекционные занятия	6
практические занятия	6
Самостоятельная работа обучающегося (всего)	60
Контрольная работа	1
Промежуточная аттестация **в форме дифференцированного зачета**	

2.2. Тематический план и содержание учебной дисциплины «Правовые основы информационной безопасности» (заочная форма обучения)

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Тема 1. Информационное общество и информационная безопасность.	**Содержание учебного материала**	-	1
	Понятие, предпосылки и характерные черты информационного общества. Стратегия развития информационного общества в РФ. Цель, задачи и принципы развития информационного общества в РФ. Контрольные значения показателей развития информационного общества в РФ. Национальные интересы РФ в информационной сфере. Основные составляющие национальных интересов РФ в информационной сфере. Внутренние и внешние угрозы информационной безопасности РФ, их источники. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности РФ.	-	
Тема 2. Законодательство РФ в области информационной безопасности.	**Содержание учебного материала**	**2**	1
	Основные этапы развития российского законодательства об информации, информатизации и защите информации. Конституция РФ, уголовное, административное, гражданское законодательство, федеральные законы и иные нормативные акты. Предмет правового обеспечения информационной безопасности. Правовое обеспечение безопасности информации в форме сведений и сообщений. Содержание и структура законодательства. Проблемы правового обеспечения и защиты информации в современной России. Перспективы развития законодательства в области информационной безопасности.	2	
	Практические занятия	-	1
	1. Анализ федеральных законов в области информационной безопасности	-	
Тема 3. Государственная система защиты информации.	**Содержание учебного материала**	**2**	1
	Организация работ по защите информации. Структура и основные функции государственной системы защиты информации. Государственные органы управления в области информационной безопасности, их права и обязанности.	2	

Тема 4. **Информация как объект правового регулирования.**	**Содержание учебного материала**	**2**	1
	Структура информационной сферы и характеристика её элементов. Понятие и виды информации. Основные признаки информации, принципиальные для правового регулирования отношений по поводу информации. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации. Информационная сфера и информационная среда. Информационная инфраструктура. Сегменты информационной инфраструктуры. Обладатель информации, его права и обязанности. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации. Ответственность в информационной сфере.	2	
Тема 5. **Правовое регулирование отношений по защите государственной тайны.**	**Содержание учебного материала**	**-**	1
	Государственная тайна как особый вид защищаемой информации. Засекречивание и рассекречивание сведений, составляющих государственную тайну; порядок распоряжения. Ответственность за нарушение режима государственной тайны.	-	
	Практические занятия	**-**	1
	1. Решение ситуационных задач.	-	
Тема 6. **Правовые режимы защиты конфиденциальной информации.**	**Содержание учебного материала**	-	1
	Правовое обеспечение защиты коммерческой тайны, персональных данных, служебной тайны, профессиональной тайны (банковская тайна, тайна следствия и судопроизводства, врачебная тайна и др.), тайны личной и семейной жизни и других тайн. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Правовые аспекты защиты информации, циркулирующей в телефонных и других линиях и системах связи. Правовое регулирование отношений предприятия с другими предприятиями, организациями и гражданами по защите конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов защиты конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).	-	
	Практические занятия	**2**	2
	1. Решение ситуационных задач	2	
Тема 7.	**Содержание учебного материала**	-	1

Защита прав на результаты интеллектуальной собственности.	Законодательство РФ об интеллектуальной собственности. Понятие интеллектуальной собственности. Объекты интеллектуальной собственности. Объекты и субъекты авторских прав. Исключительные авторские права. Смежные права. Объекты смежных прав. Правовая охрана программ для ЭВМ и баз данных. Защита авторских и смежных прав. Основы патентных правоотношений. Объекты патентных прав. Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Защита прав патентообладателей и авторов. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности.	-	
	Практические занятия	**2**	2
	1. Решение ситуационных задач.	2	
Тема 8. **Защита информации в компьютерных системах.**	**Содержание учебного материала**	-	1
	Защита информации от потери и разрушения. Защита информации от несанкционированного доступа. Пути несанкционированного доступа. Организационные меры защиты информации. Защита информации от утечки по техническим каналам. Технические каналы утечки информации. Каналы утечки речевой информации. Утечка информации по проводным коммуникациям. Основные методы, используемые при создании систем защиты информации. Основные способы защиты информации в телефонных каналах. Программные средства защиты информации. Криптографическая защита информационных ресурсов. Электронная подпись. Обеспечение защиты информации в компьютерных сетях. Угрозы безопасности сети. Службы безопасности сети. Механизмы безопасности. Организация защиты информации в корпоративной сети. Структура схемы безопасности. Этапы построения политики безопасности.	-	
Тема 9. **Преступления в сфере компьютерной информации.**	**Содержание учебного материала**	-	1
	Понятие компьютерных преступлений и их классификация. Уголовно-правовая характеристика компьютерных преступлений. Типичные цели и мотивы совершения компьютерных преступлений. Способы совершения компьютерных преступлений. Компьютерные вирусы. Жизненный цикл компьютерного вируса. Классификация компьютерных вирусов. Основные каналы распространения вирусов и других	-	

	вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ. Тенденции развития компьютерной преступности в России. Характеристика неправомерного доступа к компьютерной информации. Особенности субъектов преступления. Категории субъектов преступления. Классификация личностей преступников, совершающих неправомерный доступ к компьютерной информации. Виды хакеров. Новая и старая школы хакеров. Криминологическая характеристика мошенничеств, совершаемых с использованием сети Интернет. Усредненный «портрет» среднестатистического Интернет-мошенника. Выявление и расследование мошенничеств, совершаемых с использованием сети Интернет.		
Тема 10. Расследование преступлений в сфере компьютерной информации.	**Содержание учебного материала**	-	1
	Понятие оперативно-розыскной деятельности и оперативно-розыскных мероприятий по законодательству РФ. Органы, уполномоченные на осуществление оперативно-розыскной деятельности. Система правовых актов, регулирующих проведение оперативно-розыскных мероприятий. Криминалистические аспекты проведения расследования компьютерных преступлений. Особенности расследования преступлений в области компьютерной информации: привлечение специалистов, специфические приемы работы с машинными носителями, выдвижение и проверка следственных версий. Экспертиза преступлений в сфере компьютерной информации. Объекты компьютерно-технической экспертизы. Виды компьютерно-технических экспертиз. Группы вопросов, выносимых на разрешение компьютерно-технической экспертизы. Исследование программного обеспечения. Вопросы, разрешаемые при исследовании программного обеспечения. Исследование баз данных. Вопросы, разрешаемые при исследовании баз данных. Исследование аппаратного обеспечения ЭВМ. Вопросы, разрешаемые при исследовании аппаратного обеспечения ЭВМ.	-	
Итоговое занятие	Дифференцированный зачет	2	
	Всего	**72**	

Для характеристики уровня усвоения учебного материала используются следующие обозначения:

1 – ознакомительный (узнавание ранее изученных объектов, свойств);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3– продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета.

Оборудование учебного кабинета:

- рабочее место преподавателя;
- посадочные места по количеству студентов;
- комплект плакатов.

Технические средства обучения:

- мультимедиапроектор;
- мультимедийные презентации.

4.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бабаш, А. В. Информационная безопасность [Текст]: лабораторный практикум : учебное пособие для вузов / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — 2-е изд., стер. — Москва: КноРус, 2013. — 131 с. : ил. + 1электрон. опт. диск (CD-ROM). — (Бакалавриат). — Библиогр. в конце разд. —ISBN 978-5-406-02760-8.
2. Бачило, И.Л. Информационное право: учебник для вузов. М.: Высшее образование; Юрайт-Издат, 2012.
3. Городов, О.А. Информационnot право: учебник для бакалавров. Москва: Проспект, 2013.
4. Информационные технологии в юридической деятельности [Текст] : учебник для бакалавров / [А. А. Стрельцов и др.] ; под общ. ред. П. У. Кузнецова.— М.: Юрайт, 2012. —422 с. —(Бакалавр). —Глоссарий: с. 395-402. —Авт. указаны на с. 8. — Библиогр.: с. 403-422. —ISBN 978-5-9916-1779-6.
5. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. — 5-е изд., стер. — Москва: Академия

Дополнительные источники:

1. Галатенко В. А. Основы информационной безопасности: курс лекций: учебное пособие / В. А. Галатенко; под ред. В. Б. Бетелина. М.: ИНТУИТ, 2006.
2. Семененко В. А. Информационная безопасность: учебное пособие / В. А. Семененко. М.: МГИУ, 2006.
3. Лопатин, В.Н., Федотов М.А. Информационное право: учебник СПб.: Изд-во «Юридический центр Пресс», 2005.
4. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Мн., 2006.
5. Попов, Л.Л., Мигачев Ю.И., Тихомиров С.В. Информационное право: учебник. СПб., 2005.
6. Правовая информатика: теория и практика: учебник для бакалавров / [Т. М. Беляева и др.]; под ред. В. Д. Элькина. М.: Юрайт, 2012.

7. Рассолов, И.М. Право и интернет: теоретические проблемы. Монография. М.: Норма. 2009.

Нормативные правовые акты:

2. Окинавская хартия глобального информационного общества: Принята на о. Окинава 22.07.2000 // Дипломатический вестник. 2000. № 8. С. 51-56.

3. Конституция Российской Федерации: Принята всенародным голосованием 12.12.1993 (в посл. ред.) // СЗ РФ. 1996. № 5. Ст. 410.

4. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (в посл. ред.) // Российская газета. 1996. 6 февраля.

5. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (в посл. ред.) // Российская газета. 2006. 22 декабря.

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в посл. ред.) // СЗ РФ. 1996. № 25. Ст. 2954.

7. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (посл. ред.) // Российская газета. 2001. 31декабря.

8. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в посл. ред.) //Российская газета. 2006. 29 июля.

9. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (в посл. ред.) // Российская газета. 2004. 5 августа.

10. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ (в посл. ред.) // Российская газета. 2011. 6 мая.

11. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

12. Федеральный закон «Об оперативно-розыскной деятельности» от12.08.1995 № 144-ФЗ (в посл. ред.) // Российская газета. 1995. 18

13. Федеральный закон «О техническом регулировании» от 27.12.2002 №184-ФЗ (в посл. ред.) // Российская газета. 2002. 31 декабря.

14. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (в посл. ред.) //Российская газета. 2003. 10 июля.

15. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (в посл. ред.) // Российская газета. 2011. 8 апреля.

16. Федеральный закон «О банках и банковской деятельности» от02.12.1990 № 395-1 (в посл. ред.) // Российская газета. 1996. 10 февраля.

17. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (в посл. ред.) // СЗ РФ 1997. № 41. Стр. 8220-8235.

18. Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203 (в посл. ред.) // Российская газета. 1995. 27 декабря.

19. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 № 188 (в посл. ред.) //Российская газета. 1997. 14 марта.

20. Указ Президента РФ «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» от 30.05.2005 № 609 (в посл. ред.) // Российская газета. 2005. 7 июня.

21. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-

телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 (в посл. ред.) // СЗ РФ.2008. № 12. Ст. 1110.

22. Доктрина информационной безопасности Российской Федерации: Утв. Президентом РФ 05.12.2016 № 646 // СЗ РФ. 2016. 12 декабря.

23. Стратегия развития информационного общества в Российской Федерации: Утв. Президентом РФ 09.05.2017 № 203 // СЗ РФ. 2017. 15 мая.

24. Постановление Правительства РФ "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" от 16.04.2012 № 313 (в посл. ред.) // СЗ РФ. 2012. 23 апреля, N 17, ст. 1987.

25. Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // Российская газета. 2008. 24 сентября.

26. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119 // Российская газета. 2012. 7 ноября.

27. Постановление Правительства РФ «О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в Российской Федерации, сведений, составляющих государственную тайну» от 24.12.2007 № 928 (в посл. ред.) //Российская газета. 2007. 28 декабря.

28. Постановление Правительства РФ «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» от 06.02.2010 № 63 // СЗ РФ. 2010. № 7. Ст. 762.

29. Постановление Правительства РФ "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" от 15.04.1995 № 333 (в посл. ред.) // Российская газета. 1995. 5 мая.

30. Постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 № 79 // СЗ РФ. 2012. № 7. Ст. 863.

31. Приказ Минкомсвязи РФ «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования» от 25.08.2009 № 104 // Российская газета. 2009. 7 октября.

32. Приказ ФСБ РФ "Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению

государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" от 30.08.2012 № 440 (в посл. ред.) // Российская газета. 2012. 26 октября.

33. Приказ ФСБ РФ "Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" от 10.01.2013 № 7 (в посл. ред.) // Российская газета. 2013. 27 февраля.

34. Приказ ФСТЭК РФ «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» от 17.07.2017 № 134 (в посл. ред.) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.08.2017.

35. Приказ ФСТЭК РФ «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации» от 17.07.2017 № 133 (в посл. ред.) //Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 15.08.2017.

36. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации» от 28.12.2012 № 683 (в посл. ред.) // Российская газета. 2013. 19 апреля.

Интернет-ресурсы:

1. Информационная справочно-правовая система «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/

2. Информационная справочно-правовая система «Консультант плюс» [Электронный ресурс]. – http://base.consultant.ru /

3. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения студентами индивидуальных домашних заданий.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
умения:	
− применять действующую законодательную базу в области информационной безопасности; − анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития; − организовывать работу с персоналом, обладающим конфиденциальной информацией; − организовывать работу по обеспечению технической защиты информации с ограниченным доступом (конфиденциальной информации) на территории РФ.	Текущий контроль: контроль выполнения практических работ, контроль выполнения индивидуальных творческих заданий, тестирование, выполнение внеаудиторной самостоятельной работы. Итоговый контроль: дифференцированный зачет.
знания:	
− содержание основных понятий по правовому обеспечению информационной безопасности; − правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; − понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; − методы пресечения разглашения конфиденциальной информации; − виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений; − теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию.	Текущий контроль: индивидуальный и фронтальный опрос в ходе аудиторных занятий, контроль выполнения индивидуальных и групповых заданий, внеаудиторной самостоятельной работы. Итоговый контроль: дифференцированный зачет