Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт права и национальной безопасности
Кафедра правового обеспечения национальной безопасности

УТВЕРЖДЕНА
решением кафедра правового обеспечения
национальной безопасности
Протокол от «17» мая 2017 г. №2

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.16 Правовое обеспечение информационной безопасности

Специальность
40.05.01 Правовое обеспечение национальной безопасности

Специализация «гражданско-правовая»

Квалификация: юрист

Форма обучения: очная

Год набора-2017

Москва, 2017 г.

Автор: Мерзляков Сергей Энгельсович, кандидат юридических наук, доцент кафедры правового обеспечения национальной безопасности Юридического факультета им. М.М. Сперанского Института права и национальной безопасности

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины (модуля) в структуре образовательной программы
3. Содержание и структура дисциплины (модуля)
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю)
5. Методические указания для обучающихся по освоению дисциплины (модуля)
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю)
    6.1. Основная литература
    6.2. Дополнительная литература
    6.3. Учебно-методическое обеспечение самостоятельной работы
    6.4. Нормативные правовые документы
    6.5. Интернет-ресурсы
    6.6. Иные источники
    7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями с учетом этапов:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК ОС-4	Способность обнаруживать реальные и скрытые угрозы безопасности деятельности органов и организаций	ОПК ОС-4.1.6	способность различными способами и с применением конкретной методики проводить мероприятия по снижению уровня опасности в деятельности органов и организаций
ОПК ОС-5	Способность внедрять новые технологии и методики противодействия угрозам национальной безопасности	ОПК ОС-5.1.7	способность выделять перспективные направления в национальной безопасности и реализации проектов внедрения новаций, учитывая развитие различных информационно-коммуникационных технологий

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Профессиональные действия	**Код этапа освоения компетенции**	**Результаты обучения**
	ОПК ОС-4.1.6	**на уровне знаний:** - о различных видах безопасности и правовом регулировании деятельности по безопасности; - о видах угроз безопасности, о последствиях реализации этих угроз, о способах и методике проведения мероприятий по снижению уровня опасности в деятельности органов и организаций. - Воспроизводит основные понятия, определения и категории информационной безопасности, умеет их раскрыть, прокомментировать. Знает иерархию законодательного регулирования различных видов безопасности, называет законы и другие нормативные акты, умеет объяснить их содержание. Ориентируется в политических, экономических, социальных процессах деятельности организации, используя правовые знания, основанные на этических постулатах. Оценивает ситуации и события в деятельности организации с позиций ее безопасности. Распознает проблемы, возникающие в практической деятельности, сопряженные с угрозами информационной безопасности организации.
	ОПК ОС-5.1.7	**на уровне знаний:** о различных видах безопасности и правовом регулировании деятельности по безопасности;

		о видах угроз безопасности; о последствиях реализации этих угроз; о реализации органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов; о передовом отечественном и зарубежном опыте решения проблем безопасности; о научных разработках в этой сфере.

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Объем дисциплины

Общая трудоемкость дисциплины составляет 84 а.ч. (2 з.е.)

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

- очная форма обучения: лекции – 26 а.ч., практические занятия – 28 а.ч., самостоятельная работа – 30 ч.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.16 «Правовое обеспечение информационной безопасности» (ПОИБ) входит в базовую часть (Б.1) профессионального цикла дисциплин (Блок 1) в качестве обязательной базовой дисциплины по специальности 40.05.01 Правовое обеспечение национальной безопасности. Изучается на 5 курсе в 1-ом семестре.

Существует междисциплинарная логическая и содержательно-методическая взаимосвязь ПОИБ с другими дисциплинами профессионального цикла: теорией государства и права, конституционным правом, административным правом, уголовным правом, экологическим правом, основами теории национальной безопасности, трудовым правом. Междисциплинарная логическая и содержательно-методическая взаимосвязь БЖД существует с учебными дисциплинами гуманитарного, социального и экономического цикла:

Б1.Б.21 Уголовное право;

Б.1.Б.15 Криминология;

Криминалистика;

Административное право;

Гражданское право;

Информационное право.

«Правовое обеспечение информационной безопасности» является опорой для усвоения материала таких дисциплин, как

Б1.Б.35.04 Правовой режим охраны и гарантии национальной безопасности;

Б1.Б.35.06 Правоохранительная деятельность в сфере обеспечения национальной безопасности;

Б1.Б.35.07 Предупреждение (профилактика) криминальных угроз национальной безопасности.

Форма итоговой аттестации в соответствии с учебным планом – экзамен.

3.Содержание и структура дисциплины (модуля)

Содержание дисциплины

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КСР		
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.	5	2		2		1	**о**
Тема 2	Нормативно-правовая база обеспечения ИБ в России.	5	2		2		1	**о**
Тема 3	Информация как объект правового регулирования и защиты.	5	2		2		1	**о**
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус.	5	2		2		1	**о**
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.	5	2		2		1	**о**
Тема 6	Правовая защита личности в информационной сфере.	5	2		2		1	**о**
Тема 7	Правовой режим государственной	5	2		2		1	**о**

	тайны и меры по ее обеспечению.							
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий.	5	2		2		1	**о**
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС).	6	2		2		2	**о**
Тема 10	Правовая защита коммерческой тайны (КТ).	6	2		2		2	**о**
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации.	6	1		3		2	**о**
Тема 12	Предупреждение преступлений в информационной сфере в современной России.	6	1		3		2	**о**
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ.	8	2		4		2	**о**
Промежуточная аттестация		**36**						**экзамен**
Всего:		**108**	**24**		**30**		**18**	

Структура дисциплины

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

Понятие ИБ и информационного общества.

Цели, задачи и принципы обеспечения ИБ.

Угроза национальной безопасности и их виды.

Информационные войны и информационное оружие. Информационный терроризм.

Информационное общество в РФ и его характеристики. Информационная сфера и ее области.

Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

Понятие правового обеспечения и правовой защиты.

История формирования законодательства РФ об информации и ее защите.

Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ.

Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ.

Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения.

Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ.

Правовое регулирование деятельности средств массовой информации.

Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

Тема 3. Информация как объект правового регулирования и защиты.

Информация, ее виды и признаки.

Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды.

Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны.

Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты.

Основные принципы засекречивания информации.

Конфиденциальная информация и возможные каналы ее утечки.

Информационная инфраструктура и информационная среда. Их структура и характеристики.

Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития.

Государственная политика РФ в сфере правового обеспечения ИБ.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Понятие государственного управления в сфере обеспечения ИБ.

Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности.

Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.

Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

Понятие и виды преступности в информационной сфере.

Основные этапы и тенденции развития компьютерной преступности в России.

Особенности детерминации преступлений, совершаемых в информационной сфере.

Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет.

Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации.

Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

Особенности объективных признаков компьютерных преступлений. Основные способы их совершения.

Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения.

Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.

Конституционные гарантии правовой охраны прав личности в информационной сфере.

Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни.

Правовой механизм защиты права на неприкосновенность частной жизни.

Врачебная тайна как институт защиты интересов личности.

Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных.

Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

Понятие государственной тайны и правового режима ее обеспечения.

Принципы и механизм отнесения сведений к государственной тайне (ГТ).

Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.

Субъекты обеспечения режима государственной тайны и их правовой статус.

Организационно-правовые меры защиты ГТ.

Допуск и доступ к ГТ.

Обеспечение ИБ при международном обмене информацией.

Система контроля за режимом обеспечения ГТ.

Особенности юридической ответственности за нарушение режима обеспечения ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.

Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.

Компьютерные преступления и особенности их идентификации и предупреждения.

Правовые основы применения «электронной цифровой подписи» (ЭЦП).

Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира.

Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа.

Органы лицензирования и сертификации и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах.

Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС.

Правовой механизм обеспечения защиты авторских и смежных прав.

Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных.

Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства.

Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей.

Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак.

Программы для ЭВМ и механизм их правовой защиты.

Правовое регулирование договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

Понятие КТ и ее правовой статус.

Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель.

Объекты защиты КТ. Особенности правового обеспечения режима КТ.

Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ.

Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти.

Юридическая ответственность за нарушения режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ.

Понятие лицензирования по российскому законодательству.

Виды деятельности, подлежащие лицензированию в сфере ИБ.

Система государственного лицензирования в сфере ИБ и ее функции.

Субъекты лицензирования в сфере ИБ и их правовой статус.

Порядок лицензирования, приостановления или аннулирования действия лицензии.

Специальная экспертиза предприятия и государственная аттестация их руководителей.

Контроль за условиями обеспечения ИБ лицензиатами.

Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ.

Цели создания системы ССЗИ.

Организационная структура системы ССЗИ и особенности правового статуса ее субъектов.

Объекты сертификационной деятельности и режимы сертификации.

Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации.

Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Информационная безопасность России и задачи по ее обеспечению.

Система детерминант преступности в информационной сфере. Уровневый подход.

Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ.

Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус.

Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ.

Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ.

Зарубежный опыт борьбы с преступностью в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ.

Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.

Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России.

Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ.

Составы административных правонарушений, посягающих на ИБ страны.

Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

Вопросы для подготовки к практическим занятиям (ПЗ).

Тема 1. ИБ РФ и задачи по ее обеспечению.

1. Понятие ИБ и ее место в системе национальной безопасности России.
2. Угрозы ИБ в современной России. Особенности информационного терроризма и его место в системе угроз ИБ.
3. Национальные интересы РФ в информационной сфере и особенности реализации государственной политики России в сфере ИБ.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

1. Информационное право России, его предмет и метод.
2. Международно-правовые документы, регулирующие отношения в сфере ИБ и их место в системе НПА России.
3. Ведомственные и корпоративные нормы в системе норм, обеспечивающих ИБ РФ,

Тема 3. Информация как объект правового регулирования и защиты.

1. Основные подходы к понятию ИБ и ее виды.

2. Информация как объект правовой защиты.
3. Государственная тайна как объект правовой защиты.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

1. Система органов государственной власти РФ, обеспечивающих ИБ и право доступа к информации.
2. Правовой статус и организация работы органов государственной власти, обеспечивающих ИБ страны.
3. Задач и правовой статус службы Специальной связи и информации ФСБ РФ.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

1. Понятие и виды преступности в информационной сфере.
2. Криминологическая уголовно-правовая характеристика лиц, совершающих коммерческие преступления.

Тема 6. Правовая защита личности в информационной сфере.

1. Понятие правового механизма обеспечения прав личности в информационной сфере и его структурные составляющие.
2. Конституционные гарантии обеспечения прав личности в информационной сфере.
3. Конституционные гарантии обеспечения прав личности в информационной сфере.
4. Механизм правовой защиты персональной тайны. Виды персональной тайны.

Тема 7. Правовой режим государственной тайны (ГТ) и меры по ее обеспечению.

1. Понятие ГТ и особенности процедуры отношения сведений к ГТ и ее защиты.
2. Субъекты обеспечения ГТ и особенности их правового статуса.
3. Юридическая ответственность за

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

1. Особенности правового обеспечения защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.
2. Понятие криптографической защиты информации и способы ее обеспечения в современном мире.
3. Органы лицензирования и сертификации, и обеспечивающих защиту информации в сфере высоких технологий и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

1. Понятие ИС и правовой механизм его обеспечения в РФ.

2. Понятие патентного права и механизм правовой защиты прав автора и патентообладателя.
3. Особенности правового регулирования договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

1. Понятие КТ и особенности правового режима ее обеспечения.
2. Организационные меры обеспечения защиты КТ и особенности их реализации в различных моделях правоотношений.
3. Особенности юридической ответственности за нарушение режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

1. Понятие лицензирования и сертификации по российскому законодательству и особенности их правового регулирования.
2. Субъекты обеспечения ИБ РФ и особенности их правового статуса.
3. Основные модели предупреждения преступление в сфере ИБ р России и за рубежом. Особенности их реализации в современном мире.

Тема 13. Юридическая ответственность (ЮО) за правонарушения в сфере ИБ.

1. Понятие ЮО и ее виды в РФ.
2. Уголовная ответственность за компьютерные преступления и особенности уголовной политики России в сфере ИБ.
3. Административная ответственность за правонарушения, посягающих на ИБ России и особенности правового статуса субъектов административно-юрисдикционной деятельности.

Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю).

Этап освоения компетенции	Рекомендуемые средства (методы) оценивания	Требования к содержанию типовых оценочных средств	Элементы, которые необходимо дополнить в шкалу оценивания дисциплинарных знаний
ОПК ОС-4.1. Способен усвоить знания об основных категориях и понятиях права, его отраслей и институтов; о различных видах безопасности и правовом регулировании деятельности по	Устное собеседование	Перечень дополнительных вопросов для собеседования может включать различные варианты формулировок общего вопроса темы собеседования, либо конкретизацию отдельных частей, позиций общего вопроса.	Оценка «зачтено» выставляется обучающемуся, продемонстрировавшему, помимо дисциплинарных знаний: - грамотное, связное, логически последовательное изложение ответа на поставленные вопросы; знание специальной терминологии; умение на практических примерах показать действие теории, популярно объяснить сложные юридические коллизии. - стойкую гуманистическую нравственную позицию в оценке состояния безопасности в организации;

безопасности; о видах угроз безопасности, о последствиях реализации этих угроз, о способах и методике проведения мероприятий по снижению уровня опасности в деятельности органов и организаций			- умение связать теоретические знания с практикой, грамотно применить конкретные нормы права к смоделированным ситуациям; - умение прогнозировать последствия принимаемых решений, осознание степени и готовность нести ответственность за них в соответствии с законодательством и нравственными нормами общества. Оценка «не зачтено» выставляется обучающемуся в случае, если он: - не имеет прочных (хорошо усвоенных) знаний о различных видах безопасности и правовом регулировании деятельности по безопасности; о видах угроз безопасности, о последствиях реализации этих угроз, о способах и методике проведения мероприятий по снижению уровня опасности в деятельности органов и организаций; - с трудом разбирается в оценке факторов опасности для организации, затрудняется их описать, путается, старается угадать реакцию преподавателя; - безграмотно, несвязно, логически непоследовательно пытается ответить на поставленные вопросы; не знает специальной терминологии; не умеет на практических примерах показать действие теории, популярно объяснить специфические вопросы; - не умеет использовать методику анализа безопасности организации; - не проявляет гуманистической нравственной позиции в оценке действий физических и юридических лиц, реализующих функции безопасности в организациях.
	Доклад, презентация.	**Дополнительные требования к содержанию, визуальному ряду и защите презентации, по разработанному обучающимся докладу:** - полнота охвата тематики темы; - наличие логики в структурном оформлении тематических материалов; - наглядность: использование графических, цветовых решений, иллюстрирования,	**Оценка «отлично» (либо ее балльный аналог) выставляется обучающемуся, продемонстрировавшему при защите:** - грамотность; - навыки работы с шаблонами служебных документов; - навыки написания и редактирования юридических и служебных документов, соблюдения процедур их доработки и утверждения; - навыки деловой описательности результатов профессиональной деятельности, аргументации своей профессиональной позиции; - использование объемного словарного запаса, профессиональной терминологии; - навыки выслушивания оппонентов и

		анимационных эффектов.	формулирования содержательных ответов; **Оценка «неудовлетворительно» (либо ее балльный аналог) выставляется обучающемуся в случае, если он**: - механически списал (скопировал) презентацию доклад; - безграмотно (с явными, очевидными ошибками) оформил презентацию, доклад; - проявил неспособность устно прокомментировать отдельные аспекты своей работы; - не в состоянии отвечать на вопросы, вести полемику с оппонентами. **Преподаватель самостоятельно дополняет шкалу оценивания для оценок «хорошо» и «удовлетворительно» (либо их балльных аналогов).**
	Реферат по проблеме	**Рекомендуемый тип реферата:** информативный – целевой – текстовый. **Требования к реферату: в соответствии с ГОСТ.** **Проблемы, рекомендуемые для рассмотрения в форме реферата:** - сущность и назначение аудита безопасности в организации; - этические аспекты мониторинга безопасности текущей деятельности организации; - способы мотивации лояльности сотрудников по отношению к задачам безопасности в организации; - сканирование «медийного» и «имиджевого» образа организации как один из методов выявления скрытых угроз; - мониторинг социальных сетей с целью обеспечения кадровой безопасности; - мониторинг интернет трафика организации с позиций безопасности; - меры по борьбе с инсайдерством; - и т.п.	**Оценка «отлично» (либо ее балльный аналог) выставляется обучающемуся в том случае, если он:** - точно выполнил все формальные требования к написанию реферата; - показал глубокую теоретическую проработку темы, используя не только учебно-методическую литературу, но и научные исследования; - использовал (применил) действующее законодательство, статистические материалы; - провел параллели с практической деятельностью; - отразил собственное видение исследуемых проблем, привел собственную аргументацию в защиту своей позиции, либо выразил свое отношение к избранной им научной позиции и аргументации в ее пользу. **Оценка «неудовлетворительно» (либо ее балльный аналог) выставляется обучающемуся в случае, если он**: - проигнорировал формальные требования к написанию и оформлению реферата; - механически списал (скопировал) реферат; - безграмотно (с явными, очевидными ошибками) скомпилировал реферат; - в написании ушел от заданной темы, не раскрыл ее содержание. **Преподаватель самостоятельно дополняет шкалу оценивания для оценок «хорошо» и «удовлетворительно» (либо их балльных аналогов).**

		Рекомендуемые источники: - законодательство; - методическая литература; - данные статистики; - результаты научных исследований; - программные, отчетные и аналитические документы.	
	Коллоквиум. **Рекомендации по проведению коллоквиума с учетом дополненных тем:** - обращать особенное внимание на спорные, находящиеся в стадии решения, коллизионные вопросы; - разделять «незыблемую» теорию от вариативной практики; - проверять и поощрять умение обучающегося размышлять «вслух» над обсуждаемой темой.	**Перечень тем, выносимых на коллоквиум дополнительно к дисциплинарным темам** (примеры): 1) этапы проведения аудита безопасности; 2) ранжирование угроз; 3) роль технических средств безопасности в выявлении угроз; 4) нормативное регулирование вопросов безопасности в деятельности организации; - и т.п. **При проведении коллоквиума в форме обсуждения доклада(ов)/ реферата(ов)/проекта(ов) и других письменных работ, обучающихся содержание работы должно включать в себя описание:** - актуальности темы; - текущего состояния дел в исследуемой сфере; - законодательного регулирования исследуемой сферы; - перспективных направлений развития исследуемой сферы с позиции правового регулирования.	**Оценка «отлично» (либо ее балльный аналог) выставляется обучающемуся, продемонстрировавшему, помимо дисциплинарных знаний умение**: - вступать полемику и вести дискуссию; - применять правовые знания в ситуациях, связанных с безопасностью организации; - предвидеть последствия принятия правовых решений по вопросам безопасности организации; - толковать нормы отраслевого законодательства; - оценивать результаты предпринимаемых юридических действий; оперировать данными о состоянии законности, безопасности в деятельности организации. **Оценка «неудовлетворительно» (либо ее балльный аналог) выставляется обучающемуся в случае, если он**: - демонстрирует непонимание вопросов темы коллоквиума; - пытается отвечать без понимания сути вопроса; уходя в сторону от вопроса; - не дает ответов на прямо поставленные основные и уточняющие вопросы. **Преподаватель самостоятельно дополняет шкалу оценивания для оценок «хорошо» и «удовлетворительно» (либо их балльных аналогов).**

Этап освоения компетенции	Рекомендуемые средства (методы) оценивания	Требования к содержанию типовых оценочных средств	Элементы, которые необходимо дополнить в шкалу оценивания дисциплинарных знаний

ОПК ОС-5.1.7 способность выделять перспективные направления в национальной безопасности и реализации проектов внедрения новаций, учитывая развитие различных информационно-коммуникационных технологий	Устное собеседование.	Перечень дополнительных вопросов для собеседования может включать различные варианты формулировок общего (экзаменного) вопроса, либо конкретизацию отдельных частей, позиций общего вопроса. .	Оценка «зачтено» выставляется обучающемуся, если он: самостоятельно проводит оценку безопасности. Определяет факторы, влияющие на эффективность мер безопасности. Разделяет их на значимые и малозначимые, расставляет приоритеты в последовательности и срочности применения мер безопасности. Собирает полную информацию, позволяющую оценить уровень угрозы и опасности. Исключает недостоверную информацию. Выявляет факторы, влияющие на эффективность мер безопасности. Разделяет факторы по уровню значимости. Расставляет приоритеты в последовательности и срочности применения мер безопасности. Оценка «не зачтено» выставляется обучающемуся в случае, если он: не владеет необходимыми знаниями и навыками и не старается их применить.

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.02 Правовое обеспечение информационной безопасности используются следующие методы текущего контроля успеваемости обучающихся:

При проведении занятий лекционного типа: опрос.

При проведении практических занятий: доклад, презентация, тесты.

4.1.2. Экзамен проводится с применением следующих методов (средств): метод устного ответа на вопросы билета и дальнейшей беседы по дисциплине, а также устное решение ситуационных задач.

4.2. Материалы текущего контроля успеваемости обучающихся.

Тестовые задания

(укажите неправильный ответ).

1. К числу внешних угроз ИБ в сфере обороны относятся:

   1.1. Все виды разведывательной деятельности зарубежных государств;

   1.2. Информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

1.3. Преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем;

1.4. Диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия.

2. Для обеспечения конституционных прав и свобод человека и гражданина в области получения и пользования информацией необходимо:

2.1. Повысить эффективность информационной инфраструктуры в интересах консолидации российского общества;

2.2. Интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;

2.3. Укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности;

2.4. Обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

3. В целях обеспечения национальных интересов в сфере развития информационных технологий необходимо:

3.1. Не допускать разжигания социальной, расовой, национальной или религиозной ненависти и вражды;

3.2. Развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

3.3. Развивать и совершенствовать инфраструктуру единого информационного пространства РФ;

3.4. Обеспечить государственную поддержку фундаментальных и прикладных исследований, разработок в сфере информатизации, телекоммуникации и связи.

4. Для защиты национальных интересов в сфере защиты информационных ресурсов от несанкционированного доступа требуется:

4.1. Интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;

4.2. Обеспечить защиту сведений, составляющих государственную тайну;

4.3. Интенсифицировать формирование открытых государственных ресурсов;

4.4. Расширять международное сотрудничество в области развития и безопасного использования информационных ресурсов.

5. Угрозы информационной безопасности России в соответствии с Доктриной информационной безопасности РФ могут быть разделены на следующие виды:

5.1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности;

5.2. Угрозы информационному обеспечению государственной политики РФ;

5.3. Угрозы территориальной целостности страны, изменения правового статуса субъектов федерации;

5.4. Угрозы безопасности информационных средств и систем, как уже развернутых, так и создаваемых на территории России.

6. Основными мероприятиями по обеспечению информационной безопасности в сфере внешней политики являются:

6.1. Разработка национальных сертифицированных средств защиты информации и внедрение их в системы статистической, финансовой, биржевой, налоговой, таможенной информации;

6.2. Разработка основных направлений государственной политики в области информационного обеспечения внешнеполитического курса страны;

6.3. Совершенствование информационного обеспечения противодействия нарушения прав и свобод российских граждан и юридических лиц за рубежом;

6.4. Совершенствование информационного обеспечения РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

7. Основными мероприятиями по обеспечению информационной безопасности в сфере внутренней политики являются:

7.1. Создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

7.2. Активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России;

7.3. Блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики России;

7.4. Контроль за достоверностью информации, используемой в открытых официальных информационных ресурсах.

8. К числу внутренних угроз ИБ в сфере безопасности относится:

8.1. Деятельность иностранных политических, экономических и военных структур, направленная против интересов России;

8.2. Ненадлежащее функционирование информационных и телекоммуникационных систем специального назначения;

8.3. Преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем;

8.4. Информационно-пропагандистская деятельность, подрывающая престиж ВС РФ и их боеготовность.

9. Внутренними угрозами, представляющими наибольшую опасность для ИБ в правоохранительной сфере, являются:

9.1. Неэффективность правового регулирования информационного взаимодействия в правоохранительной сфере;

9.2. Деятельность иностранных государственных и частных структур, стремящихся получить доступ к информационным ресурсам правоохранительной системы страны;

9.3. Отсутствие защищенной системы сбора, обработки и хранения информации оперативно-розыскного характера;

9.4. Отказы технических средств и сбои программного обеспечения в информационных и коммуникационных системах.

10. Информационная безопасность в условиях чрезвычайных ситуаций обеспечивается:

10.1. Разработкой эффективной системы мониторинга объектов повышенной опасности и прогнозирования ЧС;

10.2. Подготовкой специалистов в области обеспечения ИБ в сфере обороны;

10.3. Совершенствование системы информирования населения об угрозах возникновения ЧС;

10.4. Разработка специальных мер по защите информационных систем, обеспечивающих экономически опасные производства.

11. К основным угрозам ИБ в общегосударственных информационных и телекоммуникационных системах относятся:

11.1. Использовании при создании и развитии информационных телекоммуникационных систем импортных программно-аппаратных средств;

11.2. Использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи;

11.3. Дезорганизация и разрушение системы накопления и сохранения культурных ценностей;

11.4. Привлечение к разработкам по созданию, развитию и защите информационных систем фирм, не имеющих государственных лицензий.

12. Компьютерные преступления могут быть связаны с осуществлением следующих действий:

12.1. Уничтожение или подавление каналов связи, искусственная перегрузка узлов коммуникаций;

12.2. Хищением прикладного и системного программного обеспечения;

12.3. Несанкционированным копированием, изменением или уничтожением информации;

12.4. Передачей компьютерной информации лицам, не имеющим к ей доступа.

13. Основными направлениями обеспечения ИБ в государственных информационных и телекоммуникационных системах являются:

13.1. Исключение несанкционированного доступа к обрабатываемой или хранящейся информации;

13.2. Предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

13.3. Обеспечение ИБ при подключении общегосударственных информационных и телекоммуникационных систем к внешним сетям;

13.4. Повышение специальной подготовки пользователей информационных систем.

14. Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах считаются:

14.1. Лицензирование деятельности организаций в области защиты информации;

14.2. Сертификация средств защиты информации и контроля их использования, а также защищенности информации от утечки по техническим каналам информации и связи;

14.3. Укрепление механизмов правового регулирований отношений в области распространения конфиденциальной информации;

14.4. Создание и применение информационных и автоматизированных систем управления.

15. Технические меры предупреждения компьютерной преступности предполагают:

15.1. Установку резервных систем электропитания;

15.2. Наличие плана восстановления работоспособности центра после выхода из строя;

15.3. Принятие конструктивных мер защиты от хищений диверсий;

15.4. Разработка антивирусных программ.

16. К организационным мерам предупреждения компьютерных преступлений относятся:

16.1. Защита авторских прав программистов;

16.2. Тщательный подбор персонала;

16.3. Исключение случаев ведения особо важных работ только одним человеком;

16.4. Обеспечение универсальности средств защиты всех пользователей (включая высшее руководство).

17. К правовым мерам предупреждения компьютерных преступлений можно отнести:

17.1. Совершенствование законодательства в сфере компьютерного права;

17.2. Разработка норм, устанавливающих ответственность за правонарушения на рабочих местах;

17.3. Разработка и принятие международных норм по контролю за разработчиками компьютерных программ;

17.4. Организация надежной системы архивации и дублирования наиболее ценных данных.

18. К мерам противодействия информационному терроризму можно отнести:

18.1. Создания общего центра по мониторингу угроз информационного терроризма и разработки мер быстрого реагирования;

18.2. Создание технологий обнаружения воздействия на информацию и ее защиты от несанкционированного доступа, искажения или уничтожения;

18.3. Организация качественной защиты материально-технических объектов, составляющих физическую основу информационной инфраструктуры;

18.4. Организация охраны информационного центра и введение режимных ограничений.

19. По признаку доступа информационные ресурсы делятся на:

19.1. Государственную тайну;

19.2. Коммерческую тайну;

19.3. Сведения конфиденциального характера;

19.4. Тайну исповеди.

20. К государственной тайне относятся:

20.1. Сведения о размерах имущества, денежных средств, вложениях платежей в ценные бумаги, облигации, займы, уставные фонды совместных предприятий;

20.2. Сведения о содержании стратегических и оперативных планов, о планах строительства вооруженных сил .

20.3. Сведения в области внешней политики и внешнеэкономической деятельности РФ;

20.4. Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

21. Сведениями конфиденциального характера являются:

21.1. Сведения, составляющие тайну следствия и судопроизводства;

21.2. Сведения о профессиональной деятельности (врачебная, нотариальная, адвокатская тайна и т.п.);

21.3. **Результаты научных исследований**;

21.4. Сведения о сущности изобретения или промышленных образцах до официального их опубликования.

22. Основными направлениями обеспечения безопасности в сфере духовной жизни являются:

22.1. Развитие в России основ гражданского общества;

22.2. Совершенствование информационного обеспечения противодействия нарушениям прав и свобод российских граждан за рубежом;

22.3. Совершенствование законодательства, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

22.4. Противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Темы для докладов и рефератов

1. Информационная безопасность –вечная проблема человечества.
2. Место и роль информационной безопасности в системе национальной безопасности России.
3. Информационные войны в XX веке.
4. Информационный терроризм в современном мире.
5. «Холодная» война 1945-1991 годов как информационная война.
6. Виды и источники информационных угроз.
7. Негативные последствия информационных угроз.
8. Признаки, отличающие полезную информацию от информации, являющейся средством агрессии.
9. «Непрямы» действия и «мягкие» методы информационного влияния. Их опасность для человека.
10. Внешние и внутренние угрозы информационной безопасности страны в экономике, политике, обороне, науке и технике.
11. Соотношение интересов личности, общества и государства в деле обеспечения информационной безопасности.
12. Компьютерные преступления и их опасность.
13. Язык как средство информационного манипулирования сознанием и поведением людей.
14. Связь между языком и духовностью народа.
15. Основное поле информационной битвы – умы и души людей.
16. Причины и предпосылки движения человечества к глобальному информационному обществу.
17. Позитивные и негативные стороны информационного воздействия Интернета на учащихся.
18. Угрозы информационной безопасности в глобальном мире.
19. Манипуляция сознанием и поведением людей.
20. Меры защиты от информационных манипуляций.
21. Информационные угрозы здоровью молодежи.
22. Влияние глобальной информатизации на психическое и нравственное здоровье молодежи.
23. Роль информационных технологий в деле зарождения основных видов зависимости и лечения от них.
24. Роль современной информации в деле зарождения наркотической (алкогольной, никотиновой) зависимости и освобождение от нее.

Глоссарий

1. Автоматизированная система обработки данных
2. Автор изобретения
3. Авторское право
4. Административная ответственность
5. Аттестация объектов обработки конфиденциальной информации
6. Государственная система правового обеспечения ИБ
7. Государственная тайна
8. Государственная техническая комиссия
9. Гражданско-правовая ответственность
10. Гриф секретности
11. Дисциплинарная ответственность
12. Документ
13. Засекречивание И
14. Защита И
15. Изобретательский уровень
16. Изобретения
17. Интегральная микросхема
18. Интеллектуальная собственность
19. Информатизация
20. Информационная безопасность
21. Информационная продукция
22. Информационная сфера
23. Информационное право
24. Информационно-телекоммуникационная система
25. Информационные войны
26. Информационные процессы
27. Информационные ресурсы
28. Информационные технологии
29. Информационные услуги
30. Информация
31. Исключительное авторское право
32. Источник конфиденциальной информации

33. Коммерческая тайна
34. Коммерческая тайна
35. Компьютерная И
36. Компьютерные преступления
37. Компьютерный саботаж
38. Конституционные гарантии
39. Контрафактная продукция
40. Кракер
41. Криптографическая защита
42. Лицензиат
43. Лицензионные требования и условия
44. Лицензирование
45. Лицензия
46. Материальная ответственность
47. Моральный ущерб
48. Нарушение авторских прав
49. Национальные интересы России
50. Несанкционированное использование защищенных компьютерных программ
51. Несанкционированный доступ
52. Несанкционированный доступ
53. Несанкционированный перехват данных
54. Новизна изобретения
55. Обработка персональных данных
56. Общие технические сведения
57. Основные принципы обеспечения Б
58. Патентообладатель
59. Персональные данные
60. Повреждение данных ЭВМ или программ ЭВМ
61. Подделка компьютерной И
62. Показатели патентоспособности
63. Показатель промышленной применимости
64. Полезная модель
65. Политический ущерб

66. Пользователь (потребитель И
67. Право авторства
68. Правовое обеспечение
69. Правовое регулирование
70. Правонарушения
71. Правообладатель
72. Признаки тайны
73. Программа для ЭВМ
74. Промышленный образец
75. Промышленный шпионаж
76. Разрушающие программные средства
77. Рассекречивание конфиденциальной и секретной И, работ, документов, изделий
78. Сведения особой важности
79. Секретные сведения
80. Сертификат
81. Сертификация продукции
82. Служебно-коммерческая тайна
83. Совершенно секретные сведения
84. Средства вычислительной техники
85. Стандартизация в области ИБ
86. Тайна исповеди
87. Технические средства обработки И
88. Товарный знак
89. Топология интегральной микросхемы
90. Уголовная ответственность
91. Угрозы ИБ
92. Фрикер
93. Хакер
94. Хакер-кардер
95. Экономический ущерб
96. Электрическая связь
97. Электромагнитное излучение
98. Электронная цифровая подпись

99. Юридическая ответственность

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК ОС-4	Способность обнаруживать реальные и скрытые угрозы безопасности деятельности органов и организаций	ОПК ОС-4.1.6	способность различными способами и с применением конкретной методики проводить мероприятия по снижению уровня опасности в деятельности органов и организаций
ОПК ОС-5	Способность внедрять новые технологии и методики противодействия угрозам национальной безопасности	ОПК ОС-5.1.7	способность выделять перспективные направления в национальной безопасности и реализации проектов внедрения новаций, учитывая развитие различных информационно-коммуникационных технологий

Этап освоения компетенции	Показатель Оценивания	Критерий оценивания
ОПК ОС-4.1.6: способность различными способами и с применением конкретной методики проводить мероприятия по снижению уровня опасности в деятельности органов и организаций	демонстрируется – профессиональная эрудиция в вопросах применения возможностей технических средств безопасности; – составлены организационно-правовые, справочно-информационные, справочно-аналитические документы организации по тематике безопасности	составляет: организационно-правовые, справочно-информационные, справочно-аналитические документы организации по тематике безопасности; готовит документы по личному составу, сориентированные на безопасность (кадровые, трудовые, режимные и т.п.)
ОПК ОС-5.1.7: – способность выделять перспективные направления в	определены основные направления в развитии коммуникационных, информационных и	грамотно определяет основные направления в развитии коммуникационных, информационных и высоких технологий;

Этап освоения компетенции	Показатель Оценивания	Критерий оценивания
национальной безопасности и реализации проектов внедрения новаций, учитывая развитие различных информационно-коммуникационных технологий	– высоких технологий; – описаны перспективные направления в национальной безопасности; – подготовлен проект внедрения новаций, учитывая развитие различных информационно-коммуникационных технологий	самостоятельно определяет и описывает перспективные направления в национальной безопасности; уверено проектирует внедрение инноваций в различные сферы национальной безопасности, учитывая развитие различных информационно-коммуникационных технологий

4.3.2 Типовые оценочные средства

Практические занятия

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

1. Подготовить сравнительно-правовой анализ концепций ИБ РФ и США и определить их место в системе НБ указанных стран.
2. Изобразить в виде схемы систему национальных интересов России в информационной сфере, обозначив в ней место правообеспечения ИБ.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

1. Изобразить схему правовой системы России, обозначив в ней место информационного права. Дать характеристику особенностей предмета и метода информационного права.
2. Дать характеристику международно-правовых норм и стандартов в сфере ИБ, определив их место в системе правового регулирования ИБ страны.

Тема 3. Информация как объект правового регулирования и защиты.

1. Схематично изобразить виды и источники информации, подлежащие защите в РФ.
2. Дать характеристику основным способам обеспечения защиты государственной тайны и системы контроля за состоянием ее защиты.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

1. Схематично изобразить систему органов государственной власти, обеспечивающих ИБ страны. Описать особенности их компетенции в данной сфере.
2. Охарактеризовать особенности правового статуса Службы Специальной связи и информации ФСО РФ и ее роль в обеспечении ИБ страны.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

1. Дать классификацию компьютерных преступлений. Описать особенности их объективных и субъективных признаков.

2. Создать типологию и дать криминологическую и уголовно-правовую характеристику лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

1. Дать характеристику законодательной базы России, обеспечивающей защиту прав личности в информационной сфере.

2. Раскрыть понятие персональных данных и дать их классификацию.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

1. Раскрыть понятие ГТ и назвать основные принципы отнесения сведений, имеющих конфиденциальный характер, к ГТ.

2. Раскрыть понятия «засекречивания» и «рассекречивания» информации и зафиксировать алгоритм допуска лиц к ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

1. Дать характеристику механизма правового обеспечения разработки и использования средств криптографической защиты информации.

2. Раскрыть содержание Закона РФ «Об электронной цифровой подписи» и назвать условия, при которых электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумаге.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

1. Дать определение понятия ИС и назвать основные способы ее защиты.

2. Определить особенности охраны ПИС с помощью патентов и схематично изобразить алгоритм патентования в РФ.

Тема 10. Правовая защита коммерческой тайны (КТ).

1. Дать системную характеристику нормативно-правовых актов РФ, фиксирующих механизм правовой защиты КТ, и охарактеризовать ее через систему признаков.

2. Охарактеризовать основы организации и порядок защиты КТ в различных моделях правоотношений.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

1. Схематично изобразить систему органов государственного лицензирования в сере ИБ и обозначить их полномочия.

2. Обозначить порядок проведения сертификации продукции и порядок проведения аттестации объектов информатизации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

1. Определить основы государственной политики в сфере борьбы с правонарушениями, посягающими на ИБ России. Дать характеристику оперативнорозыскных и криминалистических мероприятий, проводимых органами государственной власти в сфере обеспечения ИБ страны.

2. Дать характеристику основных моделей зарубежного опыта борьбы с правонарушениями в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

1. Дать общую характеристику института юридической ответственности за нарушение правовых норм по защите информации.
2. Охарактеризовать объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.

Вопросы к экзамену

1. Понятие информационной безопасности.
2. Цели, задачи и принципы обеспечения ИБ.
3. Угрозы ИБ. Понятие, виды.
4. Понятие и характеристика информационного общества в РФ.
5. Понятие и области информационной сферы.
6. Национальные интересы России в информационной сфере.
7. Понятие и принципы государственной политики РФ в сфере обеспечения ИБ.
8. Понятие правового обеспечения ИБ.
9. Информационное право России в структуре ее правовой системы.
10. Международно-правовые документы, регулирующие сферу ИБ. Общая характеристика и место в правовой системе РФ.
11. Средства массовой информации и их правовой статус.
12. Информация как объект юридической защиты.
13. Информационная сфера общества и ее характеристика.
14. Виды и источники информации, подлежащие защите.
15. Понятие государственной тайны и правовой режим ее защиты.
16. Способы обеспечения государственной тайны и система контроля за состоянием ее защиты.
17. Понятие и характеристики информационной структуры и информационной среды.
18. Государственная политика в сфере правового обеспечения ИБ.
19. Органы государственной власти, обеспечивающие ИБ и их правовой статус.
20. Особенности правового статуса органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.
21. Служба Специальной связи и информации Федеральной службы охраны РФ. Задачи и правовой статус.
22. Понятие и виды преступлений в информационной сфере.
23. Особенности детерминации преступлений, совершаемых в информационной сфере.
24. Компьютерные преступления. Особенности идентификации, расследования и предупреждения.

25. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.
26. Конституционные гарантии правовой охраны прав личности в информационной сфере.
27. Защита права на личную информацию с ограниченным доступом.
28. Обработка и правовая охрана персональных данных.
29. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.
30. Государственная тайна (ГТ) и правовой режим ее обеспечения.
31. Процедура засекречивания и рассекречивания сведений, составляющих ГТ.
32. Организационно-правовые меры защиты ГТ.
33. Юридическая ответственность за нарушение режима обеспечения ГТ.
34. Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.
35. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.
36. Понятие электронной цифровой подписи. «Правовые» основы ее применения.
37. Понятие криптографической защиты информации (КЗИ).
38. Правовые и организационные способы обеспечения КЗИ в России и других странах.
39. Органы лицензирования и сертификации сферы ИБ и их правовой статус.
40. Понятие интеллектуальной собственности и ее правовой статус в РФ.
41. Правовой механизм обеспечения авторских и смежных прав.
42. Правовая защита программ для ЭВМ и баз данных.
43. Правовой статус участников патентных правоотношений.
44. Механизм правовой защиты автора и патентообладателя.
45. Товарный знак и механизм его правовой защиты.
46. Правовое регулирование договорных отношений в сфере права интеллектуальной собственности.
47. Коммерческая тайна и ее правовой статус.
48. Способы правового закрепления права собственности на промышленный образец и полезную модель.
49. Организационные меры обеспечения защиты коммерческой тайны и особенности их реализации в рамках гражданско-правовых (договорных) отношений.
50. Режим представления информации, составляющей коммерческую тайну органам государственной власти.
51. Понятие лицензирования по российскому законодательству.

52. Виды деятельности, подлежащие лицензированию в сфере ИБ.
53. Система государственного лицензирования в сфере ИБ и ее функции.
54. Понятие сертификации средств защиты информации и ее правовая основа в РФ.
55. Объекты сертификационной деятельности и режимы сертификации в сфере ИБ в России.
56. Юридическая ответственности за нарушение правил лицензирования и сертификации в сфере ИБ.
57. ИБ России и задачи органов государственной власти по предупреждению деяний на нее посягающих.
58. Применение уровневого подхода к анализу системы детерминант преступности в информационной сфере.
59. Оперативно-розыскные и криминалистические мероприятия в борьбе с преступлениями в сфере ИБ.
60. Понятие и виды юридической ответственности за правонарушения в сфере ИБ.
61. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности.
62. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.
63. Уголовная ответственность за компьютерные преступления и особенности ее реализации в современной России.
64. Составы административных правонарушений, посягающих на ИБ страны.
65. Особенности производства по делам об административных правонарушениях, посягающих на ИБ.
66. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

4.4. Методические материалы

Оценивание обучающихся в процессе поэтапного освоения ими компетенций, формируемых данной дисциплиной осуществляется в форме экзамена, который предполагает оценивание знаний с помощью устного собеседования по узловым вопросам.

К экзамену допускаются студенты, выполнившие все требования учебной программы, выполнившие в установленные сроки все виды заданий и работ, не имеющим задолженностей по итогам текущего контроля успеваемости.

Подготовка к экзамену предусматривает устное повторение пройденного учебного материала по дисциплине (с использованием конспектов, учебных пособий,

дополнительной литературы), а также дополнительное конспектирование этих источников по перечню вопросов, выносимых на экзамен.

Экзамен принимает лектор.

Оценивание обучающегося на экзамене по дисциплине

Оценка	Критерии оценки	Результаты обучения
отлично	Глубокие и прочные знания теоретических основ дисциплины, свободное владение терминологией Знание взаимосвязи теории и практики, свободно справляется с задачами, вопросами и другими видами применения теоретических знаний. При видоизмении задачи затруднений не возникает. Применяются нестандартные варианты решений. Соблюдает нормы речи, ответ четкий и логически выстроен	ОПК ОС-4.1.6 на уровне знаний: - о различных видах безопасности и правовом регулировании деятельности по безопасности; - о видах угроз безопасности, о последствиях реализации этих угроз, о способах и методике проведения мероприятий по снижению уровня опасности в деятельности органов и организаций. - Воспроизводит основные понятия, определения и категории информационной безопасности, умеет их раскрыть, прокомментировать. Знает иерархию законодательного регулирования различных видов безопасности, называет законы и другие нормативные акты, умеет объяснить их содержание. Ориентируется в политических, экономических, социальных процессах деятельности организации, используя правовые знания, основанные на этических постулатах. Оценивает ситуации и события в деятельности организации с позиций ее безопасности. Распознает проблемы, возникающие в практической деятельности, сопряженные с угрозами информационной безопасности организации. ОПК ОС-5.1.7 на уровне знаний: - о различных видах безопасности и правовом регулировании деятельности по безопасности; - о видах угроз безопасности; - о последствиях реализации
хорошо	твердые знания материала, изложение грамотное и по существу, не допускаются существенных неточностей в ответе, в использовании терминологии возникают. Правильно применяет теоретические положения при решении практических вопросов и задач. Ответ четкий, но логическая последовательность ответа нарушена	
удовлетворительно	знания только основного материала, не усвоены детали, допускаются неточности, недостаточно правильные формулировки терминов и законов. Затруднения при выполнения практических работ, поиске ответов на практические вопросы, существенные затруднения при использовании терминологии. Логическое построение изложения	

	выстроена слабо	этих угроз; - о реализации органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов; - о передовом отечественном и зарубежном опыте решения проблем безопасности; - о научных разработках в этой сфере.
неудовлетворительно	Значительная часть теоретического материала не усвоена, допускаются существенные ошибки в ответе. Нормы речи отсутствуют, логическое построение изложения материала отсутствует.	

5. Методические указания обучающимся по освоению дисциплины (модуля). Формы контроля.

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на переэкзамен соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

5.1. Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

5.2. Лекции

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

5.3. Практические занятия

Практические занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на практических занятиях оценивается по следующим критериям:

- ответы на вопросы, предлагаемые преподавателем;
- участие в дискуссиях;
- выполнение проектных и иных заданий;
- ассистирование преподавателю в проведении занятий.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

5.4. Самостоятельная работа студента

Для успешного усвоения курса обучающиеся обязаны посещать аудиторные занятия (не менее половины отведенного времени), и вести активную самостоятельную работу. При самостоятельной проработке курса обучающиеся должны:

- просматривать основные определения и факты;
- повторять законспектированный на лекционном занятии материал и дополнять его с учетом рекомендованной по данной теме литературы;
- изучать рекомендованную основную и дополнительную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;
- самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;
- использовать для самопроверки материалы фонда оценочных средств;
- выполнять домашние задания по указанию преподавателя.

Домашнее задание оценивается по следующим критериям:

- степень и уровень выполнения задания;
- аккуратность в оформлении работы;
- использование специальной литературы;
- сдача домашнего задания в срок.

Оценивание домашних заданий входит в накопленную оценку.

5.5. Реферат

Реферат — индивидуальная письменная работа обучающегося, предполагающая изложение современной литературы по определенному вопросу либо проблеме.

Реферат имеет стандартную структуру: титульный лист, содержание, введение, основное содержание темы, заключение, список использованных источников, приложения.

Оценивается оригинальность темы реферата, актуальность и полнота использованных источников, системность излагаемого материала, логика изложения и убедительность аргументации, оформление, своевременность срока сдачи, защита реферата перед аудиторией.

При своевременной защите работа оценивается наивысшим баллом, при опоздании на 1 неделю балл снижается на 2, при опоздании на 2 недели балл снижается еще раз на 2. При опоздании более чем на 2 недели работа не оценивается.

Оценивание реферата входит в экзаменную оценку.

5.6. Методические рекомендации по подготовке к лекционным и семинарским занятиям

Курс дисциплины «Правовое обеспечение информационной безопасности» преподается с целями:

- ознакомления обучающихся с нормативными актами, регулирующими информационную безопасность государства; концептуальными и практическими документами, определяющими состояние дел в этой сфере, являющейся важной частью национальной безопасности Российской Федерации;
- изучения и понимания обучающимися реальных угроз информационной безопасности страны в конкретных исторических условиях; проблем безопасности, возникающих по мере развития общества, государства;
- подготовки специалистов с широкой профессиональной ориентацией, способных мыслить масштабно, грамотно взаимодействовать с представителями других сфер общественной деятельности.

Актуальность изучения курса обусловлена повышением роли стратегического планирования в сфере государственного и общественного развития, необходимостью конструктивного взаимодействия в этой сфере сил обеспечения общественной безопасности и институтов гражданского общества, определяемой Стратегией национальной безопасности Российской Федерации до 2020 года, Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, Концепцией общественной безопасности в Российской Федерации, утвержденной Президентом РФ 20 ноября 2013 года.

Исходя из целей курса, в процессе изучения дисциплины решаются следующие задачи:

- **формирование** у обучающихся знаний основных категорий и понятий информационной безопасности, а также основных положений действующего законодательства РФ и нормативных актов, регулирующих отношения в данной сфере;
- **ознакомление** с различными формами ответственности за правонарушения в сфере информационной безопасности.
- **развитие** у обучающихся навыков работы в условиях повышенной опасности и в чрезвычайных ситуациях.

В самом начале освоения дисциплины необходимо ознакомиться со следующей учебно-методической документацией:

- рабочей программой дисциплины «Правовое обеспечение информационной безопасности»;
- перечнем знаний, умений которыми обучающийся должен овладеть,
- тематическими планами занятий,
- контрольными мероприятиями,
- учебником, учебными пособиями, а также электронными ресурсами,
- перечнем экзаменационных вопросов и заданий.

Цель ознакомления - получить четкое представление об объеме и характере знаний, умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение

заданий учебной работы на лекциях и семинарских занятиях позволяет успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

К экзамену по дисциплине «Правовое обеспечение информационной безопасности» необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают неудовлетворительные результаты.

Обучение по дисциплине «Правовое обеспечение информационной безопасности также консультации) и самостоятельную работу обучающихся, в связи с чем предполагается следующая последовательность в подготовке обучающихся к лекции:

- ознакомление с материалом предыдущей лекции;
- знакомство с тематикой предстоящей лекции (по тематическому плану, представленному в настоящей рабочей программе дисциплины);
- прочтение и анализ учебных пособий, учебников, научных статей по теме предстоящего лекционного занятия;
- подготовить вопросы, которые вы предполагаете задать лектору по проблеме предстоящей лекции.

Цель практических занятий заключается в углубленном освоении лекционного материала с учетом самостоятельной подготовительной работы обучающихся. При подготовке к практическим занятиям обучающиеся:

- изучают материалы лекции по теме занятия;
- дополняют изучение лекции чтением учебно-методической литературы;
- знакомятся с вопросами, соотносящимися с темой практического занятия;
- готовят вопросы преподавателю в рамках изучаемой темы.

Обсуждение лекционного материала производится применительно к экзаменационным вопросам.

Обучающийся допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине в объеме не менее половины времени посещения лекционных и практических занятий. В случае наличия учебной задолженности обучающийся отрабатывает пропущенные занятия в форме, предложенной преподавателем.

5.7. Оценивание по дисциплине

- Накопленная оценка проставляется за активность обучающегося на практических занятиях, прохождение текущего контроля и выполнение самостоятельной работы.
- Оценка итогового контроля проставляется за прохождение контрольного испытания по курсу в формате, определенным рабочим учебным планом.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет, учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Основная литература

1. В.П. Петров, С.В. Петров «Информационная безопасность в истории и современной жизнедеятельности.»: учебно-методическое пособие / М.: ЮОУО ДО г. Москвы , 2007.

2. Лопатин В.Н. Концептуальные основы развития российского законодательства в области обеспечения информационной безопасности // Компьютерная преступность и информационная безопасность / Под общ. Ред. А.П.Леонова. – Минск : АРИЛ, 2000

3. Мельников В. П., Клейменов С. А., Петраков А. М.. Информационная безопасность и защита информации. Издательство: Академия, 2009 г. 336 с;

4. Минаев В. А., Фисун А. П.. Правовое обеспечение информационной безопасности. Издательство: Маросейка, 2008 г.;

5. Расторгуев С. П. Основы информационной безопасности. Издательство: Академия, 2007 г. 192 с;

6. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с;

7. С.Н.Семкин А.Н. Семкин Основы правового обеспечения защиты информации. М.:Горячая линия –Телеком, 2007

8. Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. 2005 г. 304 с;

9. Яковец Е.Н. Правовые основы информационной безопасности. М.: Юрлитинформ, 2010

6.2. Дополнительная литература

1. Белопушкин В.И., Кириллычев А.Н. Правовые аспекты обеспечения информационной безопасности. М., МГТУ, 2003 г.;

2. Верещагин Д. Влияние: Система дальнейшего энергоинформационного развития. – Спб: Изд-во «Невский проспект».

3. Волчинская Е.К. О стратегии и проблемах развития законодательства в сфере обеспечения информационной безопасности. Материалы конференции «Инфофорум». – 2004

4. Государственная тайна в Российской Федерации: учебно-методическое пособие / Под ред. чл.-кор. Международной академии информатизации М.А.Вуса. – Издательство С.-Пб. Университета, 1999

5. Доктрина информационной безопасности Российской Федерации. 2004 г. 48 с;

6. Замятин А., Замятин В., Юсупов Р. Опасности информационно-психологической войны. // «ОБЖ. Основы безопасности жизни» №6 2002

7. Извеков Н.Н. Исторические традиции как средство укрепления национального иммунитета в информационных войнах III тысячелетия. // Информационный сборник «Безопасность». №№7-12 2001

8. Информационная безопасность. Information Security. Издательство: Оружие и технологии России, 2009 г. 256 с;

9. Кавеладзе И.Т. Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации). – М.: Изд-во «ЭКО –консалтинг», 1992

10. Кара-Мурза С.Г. Манипуляция сознанием в России сегодня. – М.: Изд-во «Эксмо», 2001

11. Лепехин А. Н.. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. Издательство: Тесей, 2008 г. 176 с;

12. Одинцов А. А.. Защита предпринимательства (экономическая и информационная безопасность). Учебное пособие. Издательство: Международные отношения, 2003 г. 328 с;

13. Панарин И.Н., Панарина Л.Г. Информационная война и мир. – М.: Изд-во «ОЛМА-ПРЕСС», 2003

14. Петров В. П., Петров С. В. Информационная безопасность человека и общества. Издательство: НЦ ЭНАС, 2007 г.;

15. Родионов М.А. Информационное противоборство: история и современность. // Информационный сборник «Безопасность».№№7-8 2002

16. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. – М.: “Дашков и К”, 2006 г.

17. Семененко В.А. Информационная безопасность. Учебное пособие. – М.: МГИУ, 2006. – 277 с;

18. Семкин С.Н., Семкин А.Н. Основы правового обеспечения информационной безопасности. – М.: Труд, 2003

19. Тихонов В. А., Райх В. В. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. Издательство: Гелиос АРВ, 2007 г.;

20. Уманский С.В. Психологическое воздействие: манипуляция или психотерапия. В кн. «Психологическая теория и практика в изменяющейся России» (Тезисы окладов Всероссийской научной конференции). – Челябинск: Изд-во ЮУрГУ, 2006

21. Шершнев Л.И. Четвертая мировая война и ее особенности. // «ОБЖ. Основы безопасности жизни». №7,9 2005.

22. Ярочкин В. И.. Информационная безопасность. Учебник для вузов. Издательства: Академический проект, Мир, 2008

6.4. Основные нормативно-правовые документы

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

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

3. Гражданский кодекс Российской Федерации (часть вторая) от26.01.1996 № 14-ФЗ (в посл. ред.) // Российская газета. 1996. 6 февраля.

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

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

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

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

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

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

10. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в посл. ред.) // Российская газета. 2006. 29 июля.

11. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (в посл. ред.) // Российская газета. 1995. 18 августа.

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

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

14. Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ (в посл. ред.) // Российская газета. 2002. 12 января.

15. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1(в посл. ред.) // Российская газета. 1996. 10 февраля.

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

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

18. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 № 188 (в посл. ред.) // Российская газета. 1997. 14 марта.
19. 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.
20. 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.
21. Доктрина информационной безопасности Российской Федерации: Утв. Президентом РФ 09.09.2000 № Пр-1895 // Российская газета. 2000. 28 сентября.
22. Стратегия развития информационного общества в Российской Федерации: Утв. Президентом РФ 07.02.2008 № Пр-212 // Российская газета. 2008. 16 февраля.
23. Постановление Правительства РФ «Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» от 29.12.2007 № 957 (в посл. ред.) // СЗ РФ. 2008. № 2. Ст. 86.
24. 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.
25. Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 № 781 // Российская газета. 2007. 21 ноября.
26. 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.
27. 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.
28. 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.
29. Постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 № 79 // СЗ РФ. 2012. № 7. Ст. 863.
30. 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.
31. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем» от 24.06.2009 № 286 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 38.
32. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по выявлению электронных устройств, предназначенных

для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» от 24.06.2009 № 287 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 38.

33. Приказ ФСТЭК РФ «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации» от 28.08.2007 № 181 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 45.
34. Приказ ФСТЭК РФ «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации» от 28.08.2007 № 182 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 45.
35. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации» от 01.04.2009 № 123 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 29.
36. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию 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 27.02.2009 № 75 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 20.
37. Приказ МВД РФ № 368, ФСБ РФ № 185, ФСО РФ № 164, ФТС РФ № 481, СВР РФ № 32, ФСИН РФ № 184, ФСКН РФ № 97, Минобороны РФ № 147 от 17.04.2007 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю, прокурору или в суд» // Российская газета. 2007. 16 мая.
38. Приказ ФСС РФ «О внедрении защищенного обмена документами в электронном виде с применением электронной цифровой подписи для целей обязательного социального страхования» от 12.02.2010 № 19 (в посл. ред.) // СПС «КонсультантПлюс».
39. Приказ ФНС РФ «Об утверждении Унифицированного формата транспортного контейнера при информационном взаимодействии с приемными комплексами налоговых органов по телекоммуникационным каналам связи с использованием электронной цифровой подписи» от 09.11.2010 № ММВ-7-6/535@ (в посл. ред.) // СПС «КонсультантПлюс».
40. Приказ ФНС РФ «Об утверждении Требований к сертификату ключа подписи и списку отозванных сертификатов для обеспечения единого пространства доверия сертификатам ключей электронной цифровой подписи» от 02.07.2009 № ММ-7-6/353@ (в посл. ред.) // СПС «КонсультантПлюс».
41. Приказ Минкомсвязи РФ «Об утверждении Административного регламента предоставления Федеральным агентством по информационным технологиям государственной услуги по подтверждению подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей» от 10.07.2009 № 92 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 45.

42. Приказ ФНС РФ «Об утверждении Порядка ведения единого пространства доверия сертификатам ключей ЭЦП» от 17.12.2008 № ММ-3-6/665@ // СПС «КонсультантПлюс».
43. Приказ ФСТЭК РФ «Об утверждении Положения о методах и способах защиты информации в информационных системах
персональных данных» от 05.02.2010 № 58 // Российская газета. 2010. 5 марта.
44. Приказ Минкомсвязи РФ «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных» от 30.01.2010 № 18 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2010. № 16.
45. Приказ ФСТ РФ «Об утверждении Положения о работе с персональными данными государственного гражданского служащего ФСТ России и ведении его личного дела» от 07.11.2008 № 441-к (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 2.
46. Приказ Минкомсвязи РФ «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» от 14.11.2011 № 312 // СПС
«КонсультантПлюс».

6.5. Интернет ресурсы

1. http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/b46904541430deb3c3256c4e003844b5
2. http://jurisprudence.club/informatsionnoe-pravo_703/sistema-pravovogo-obespecheniya.html
3. http://law.edu.ru/book/book.asp?bookID=1288184
4. http://xn----7sbabeyocb2bkdagddhcqh9acx1a8cxksc.xn--80afh5aqv.xn--p1ai/

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Специализированные залы для проведения лекций и аудитории для проведения семинарских и практических занятий с использованием мультимедийного оборудования и возможностью прямого выхода в сеть Интернет.

2. Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами.

3. Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.

4. Лицензионные электронные ресурсы: Windows, Microsoft Office (Excel, InfoPath, PowerPoint, Publisher, Word).