

**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 кафедры правового обеспечения
национальной безопасности
Протокол от «17» мая 2017 г. №2

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Б1.Б.35.08 «Правовые основы борьбы с криминальными угрозами
информационной безопасности»**

Специальность 40.05.01

«Правовое обеспечение национальной безопасности»

Специализация «Уголовно-правовая»

Квалификация выпускника: юрист

Очная
(форма обучения)

Год набора 2016г.

Москва, 2016 г.

Автор:

доцент кафедры основ правоохранительной деятельности И.М. Хапаев

Заведующий кафедрой правового обеспечения национальной безопасности, к.ю.н.
Куражов А.В.

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы.....	4
2. Объем и место дисциплины (модуля) в структуре ОП ВО.....	7
3. Содержание и структура дисциплины (модуля).....	8
3.1. Структура дисциплины.....	8
3.2. Содержание дисциплины (модуля).....	9
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю).....	11
4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.....	11
4.2. Материалы текущего контроля успеваемости обучающихся.....	11
4.3. Оценочные средства для промежуточной аттестации.....	15
4.4. Методические материалы.....	23
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	24
5.1. Методические рекомендации по подготовке к лекционным и семинарским занятиям.....	26
5.2. Методические рекомендации к самостоятельной работе.....	29
5.3. Методические рекомендации для подготовки к опросам по вынесенным на обсуждение темам.....	30
5.4. Методические рекомендации по решению ситуационных задач и кейс-заданий.....	31
5.5. Методические рекомендации по выполнению тестовых заданий.....	31
6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю).....	33
6.1. Основная литература.....	33
6.2. Дополнительная литература.....	33
6.3. Учебно-методическое обеспечение самостоятельной работы.....	33
6.4. Нормативные правовые документы.....	37
6.5. Интернет-ресурсы.....	39
6.6. Базы данных, информационно-справочные и поисковые системы.....	40
6.7. Иные источники.....	40
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы.....	41

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

Дисциплина «Правовые основы борьбы с криминальными угрозами информационной безопасности» обеспечивает овладение следующими компетенциями с учетом этапов:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	способность применять проектный подход при решении профессиональных задач	УК ОС-2.1.5	способность осуществлять анализ правотворческой деятельности органов власти, оценивать её соответствия государственной политике Российской Федерации в сфере развития и использования информационных технологий
ПСК-1	способность выявлять возможные угрозы новых форм противоправной деятельности с применением информационно-коммуникационных и высоких технологий	ПСК-1.1.2	способность применять в профессиональной деятельности законодательство, регулирующее общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере, а также использовать современные информационно-коммуникационные и высокие технологии в противодействии транснациональной организованной преступности
ОПК ОС-5	способность внедрять новые технологии и методики противодействия угрозам национальной безопасности	ОПК ОС-5.1.6	способность принимать эффективные управленческие и правовые решения по противодействию угрозам национальной безопасности
ПК-9	способность выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения	ПК-9.3.2	способность соблюдать законодательство Российской Федерации в целях предотвращения коррупциогенных явлений, затрудняющих раскрытие преступления и иных правонарушений
ПК-10	способность применять в профессиональной деятельности теоретические основы раскрытия и расследования преступлений, использовать в целях установления объективной истины по конкретным делам технико-криминалистические методы и средства, тактические	ПК-10.2.1	способность применять юридические технологии, криминалистическую технику и методику в деятельности по выявлению, пресечению, раскрытию и расследованию преступлений и иных правонарушений

	приемы производства следственных действий, формы организации и методику раскрытия и расследования отдельных видов и групп преступлений		
ПК-11	способность реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	ПК-11.2.1	способность разрабатывать систему мер профилактики и предупреждения экономических и информационных угроз

В результате освоения дисциплины у студентов должны быть сформированы:

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
предупреждение, раскрытие, расследование преступлений	УК ОС-2.1.5	на уровне знаний: – пределов своей компетенции и основных компетенций взаимодействующих структур, практики и стереотипов принятия управленческих решений, планирования, документирования проектной деятельности
		на уровне умений: – осуществлять исполнительскую, организационно-управленческую деятельность и нести за нее ответственность с позиций социальной значимости принимаемых решений в профессиональной сфере и соответствия их правовым и этическим нормам
предупреждение, раскрытие, расследование преступлений	ПСК-1.1.2	на уровне знаний: – об основных положениях, их назначении и политико-правовой основе стратегии развития информационного общества в Российской Федерации
		на уровне умений: – применять в обеспечении информационной и национальной безопасности современные информационные, телекоммуникационные и иные высокие технологии
предупреждение,		на уровне знаний: – о видах угроз безопасности; – о последствиях реализации этих угроз

раскрытие, расследование преступлений	ОПК ОС-5.1.6	на уровне умений: – объективно оценивать влияние внешних и внутренних угроз на состояние национальной безопасности; – выделять ключевые факторы опасности и выстраивать приоритетность мер реагирования на них, применяя передовой отечественный и зарубежный опыт
предупреждение, раскрытие, расследование преступлений	ПК-9.3.2	на уровне знаний: – особенностей предупреждений и профилактики отдельных видов правонарушений и преступлений; – положений и норм законодательства по вопросам предупреждения и профилактики правонарушений и преступлений на уровне умений: – соблюдать требования законности при выявлении и устранении причин и условий правонарушений и преступлений
предупреждение, раскрытие, расследование преступлений	ПК-10.2.1	на уровне знаний: – правовых и научных основ применения технико-криминалистических средств и методов выявления, пресечения, раскрытия и расследований преступлений и иных правонарушений на уровне умений: – применять научно обоснованные средства и методы криминалистической идентификации
предупреждение, раскрытие, расследование преступлений	ПК-11.2.1	на уровне знаний: – системы мер предупреждения, пресечения, раскрытия и расследования преступлений на уровне умений: – применять знания юридической техники в целях раскрытия, пресечения и профилактики правонарушений и преступлений

2. Объем и место дисциплины (модуля) в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 72 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 – 18 а.ч., практические занятия – 18 а.ч., самостоятельная работа – 36 ч.

Место дисциплины в структуре ОП ВО

Дисциплина «Правовые основы борьбы с криминальными угрозами информационной безопасности» относится к обязательным дисциплинам базовой части профессионального цикла. Изучается студентами в 8 семестре на 4 курсе.

Для освоения дисциплины «Правовые основы борьбы с криминальными угрозами информационной безопасности» обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения предметов:

- «Теория государства и права»;
- «Правоохранительные органы»;
- «Уголовное право»;
- «Криминология»;
- «Криминалистика».

Форма промежуточной аттестации в соответствии с учебным планом – зачёт.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины

Таблица 1.

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемост и промежуточ ной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Понятие и место информационной безопасности в системе национальной безопасности России	14	4		4		6	О, КЗ, Т
Тема 2	Информационная безопасность как объект уголовно-правовой защиты	14	4		4		6	О, КЗ, Т
Тема 3	Уголовно-правовые меры защиты ин- формационной безопасности личности	14	4		4		6	О, КЗ
Тема 4	Уголовно-правовые меры защиты от криминальных угроз безопасности информации, охраняемой законом	10	2		2		6	О, КЗ, Т
Тема 5	Уголовно-правовые меры защиты безопасности в сфере высоких информаци- онных технологий	10	2		2		6	О, КЗ
Тема 6	Уголовно-правовые меры защиты от угроз информационного терроризма	10	2		2		6	О, КЗ
Промежуточная аттестация		Зачет						
Всего:		72	18		18		36	

Примечание 1. Формы текущего контроля успеваемости: опрос (О), кейсы задания (КЗ), тесты (Т)

3.2. Содержание дисциплины (модуля)

Тема 1. Понятие и место информационной безопасности в системе национальной безопасности России

Понятие информационной безопасности. Место информационной безопасности в системе национальной безопасности.

Виды угроз информационной безопасности. Источники угроз информационной безопасности Российской Федерации.

Система обеспечения информационной безопасности Российской Федерации.

Силы обеспечения информационной безопасности. Средства обеспечения информационной безопасности.

Правовая база нормативно-правовых источников обеспечения информационной безопасности Российской Федерации.

Тема 2. Информационная безопасность как объект уголовно-правовой защиты

Уголовно-правовая характеристика информационной безопасности. Общая характеристика методов обеспечения информационной безопасности РФ. Общие методы обеспечения информационной безопасности.

Понятие правовых методов обеспечения информационной безопасности. Уголовно-правовые методы обеспечения информационной безопасности. Организационно-технические методы обеспечения информационной безопасности.

Тема 3. Уголовно-правовые меры защиты информационной безопасности личности

Уголовно-правовая характеристика нарушения неприкосновенности частной жизни.

Уголовно-правовая характеристика незаконного оборота специальных технических средств, предназначенных для негласного получения информации.

Уголовно-правовая характеристика нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Тема 4. Уголовно-правовые меры защиты от криминальных угроз безопасности охраняемой законом информации

Сведения, составляющие государственную, коммерческую или иную охраняемую законом тайну.

Уголовно-правовая характеристика преступных угроз безопасности охраняемой законом информации.

Уголовно-правовая характеристика разглашения государственной тайны.

Уголовно-правовая характеристика утраты документов, содержащих государственную тайну.

Тема 5. Уголовно-правовые меры защиты безопасности в сфере высоких информационных технологий

Уголовно-правовая характеристика преступных угроз информационной безопасности.

Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.

Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ.

Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Тема 6. Уголовно-правовые меры защиты от угроз информационного терроризма

Формы уголовно-наказуемого информационного терроризма.

Уголовная ответственность за акт терроризма в форме угрозы совершения террористических действий. Уголовно-правовая характеристика угрозы совершения террористических действий.

Уголовная ответственность за заведомо ложное сообщение об акте терроризма. Уголовно-правовая характеристика заведомо ложного сообщения об акте терроризма.

Отличие заведомо ложного сообщения об акте терроризма от преступлений со смежными составами.

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

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

В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся:

- опросы по вынесенным на обсуждение темам;
- решение кейсы-задания;
- решение заданий в тестовой форме.

Зачет проводится с применением следующих методов (средств):

- метод устного ответа на вопросы билета и дальнейшей беседы по правовым нормам, а также устное решение ситуационных задач либо проблемных заданий.

4.2. Материалы текущего контроля успеваемости обучающихся

Типовые оценочные материалы по теме 1. Понятие и место информационной безопасности в системе национальной безопасности России

Вопросы к опросу:

- 1) Цели государственной информационной политики.
- 2) Предмет информационно-правового регулирования.
- 3) Задачи обеспечения информационной безопасности РФ.
- 4) Основные направления государственной информационной политики в области информационных ресурсов.
- 5) Основные элементы информация.
- 6) Понятие информационной безопасности.
- 7) Субъекты государственной политики в области информационной безопасности.

Кейс-задания:

1. Сформулируйте принципы государственной политики обеспечения информационной безопасности.
2. Дайте подробную характеристику национальных интересов в информационной сфере, классифицируйте их.
3. Определите и классифицируйте угрозы информационной безопасности Российской Федерации.

Типовые оценочные материалы по теме 2. Информационная безопасность как объект уголовно-правовой защиты

Вопросы к опросу:

- 1) Дайте определение понятию «информация».
- 2) Назовите формы представления информации.
- 3) Перечислите свойства информации.
- 4) Охарактеризуйте правовые режимы информации.
- 5) Какие методы обеспечения информационной безопасности вы знаете?
- 6) Перечислите уголовно-правовые методы обеспечения информационной безопасности.
- 7) Укажите организационно-технические методы обеспечения информационной безопасности РФ.

Кейс-задания:

1. Раскройте сущность института уголовно-правовой защиты информационной безопасности.
2. Разработайте правовые методы защиты информации по следующим направлениям:
 - а) защита прав личности на частную жизнь;
 - б) защита государственных интересов;
 - в) защита предпринимательской и финансовой деятельности.

Типовые оценочные материалы по теме 3. Уголовно-правовые меры защиты информационной безопасности личности

Вопросы к опросу:

- 1) Понятие персональных данных.
- 2) В чем различие между понятиями «персональные данные», «персонифицированная информация»?
- 3) Какие органы государственной власти обеспечивают охрану конфиденциальной информации?
- 4) Определите соотношение понятий «сведения о частной жизни», «тайна личной жизни», «сведения об интимных сторонах жизни лица», «личная и семейная тайна».

Кейс-задание:

Изучите российское законодательство в сфере обеспечения информационной безопасности. Определите систему нормативных актов, регламентирующих информационно-правовые отношения интеллектуальной собственности.

Типовые оценочные материалы по теме 4. Уголовно-правовые меры защиты от криминальных угроз безопасности информации, охраняемой законом

Вопросы к опросу:

- 1) Назовите виды информационных ресурсов по принадлежности и по доступности.
- 2) Дайте определение общедоступных и конфиденциальных персональных данных.
- 3) Существует ли информация, которую запрещено относить к информации ограниченного доступа?
- 4) Назовите органы, осуществляющие контроль за соблюдением требований к защите информации.
- 5) Кем определяется характер и объем информации, составляющей ту или иную тайну?

Кейс-задание:

По признакам объективной стороны состава преступления классифицируйте преступления в информационной сфере.

Типовые оценочные материалы по теме 5. Уголовно-правовые меры обеспечения безопасности в сфере высоких информационных технологий

Вопросы к опросу:

- 1) Какая информация называется компьютерной?
- 2) Что является неправомерным доступом к компьютерной информации?
- 3) Раскройте понятие «вредоносной программы».
- 4) Какие действия предполагают нарушение правил эксплуатации ЭВМ?

Кейс-задания:

1. Сформулируйте вопросы для технической экспертизы, назначаемой при расследовании преступлений в сфере высоких информационных технологий.
2. Предложите классификацию преступлений в сфере информационных технологий.

Типовые оценочные материалы по теме 6. Уголовно-правовые меры защиты от угроз информационного терроризма

Вопросы к опросу:

- 1) Дайте понятие «информационного терроризма».

- 2) Раскройте теорию «информационной войны».
- 3) Перечислите виды «информационного терроризма».
- 4) Классификация наиболее уязвимых (по отношению к информационному нападению) технологий, систем и структур.
- 5) Назовите основные направления стратегии противодействия «информационному терроризму».

Кейс-задания:

1. В соответствии с «Доктриной информационной безопасности Российской Федерации» от 05.12.2016 дайте характеристику методам обеспечения информационной безопасности в Российской Федерации.

2. На примере любого субъекта Российской Федерации постройте систему органов государственной власти субъекта РФ, имеющих полномочия в области обеспечения права граждан на доступ к информации. Укажите со ссылками на нормативные правовые акты субъектов РФ данные полномочия.

4.3. Оценочные средства для промежуточной аттестации

Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	способность применять проектный подход при решении профессиональных задач	УК ОС-2.1.5	способность осуществлять анализ правотворческой деятельности органов власти, оценивать её соответствия государственной политике Российской Федерации в сфере развития и использования информационных технологий
ПСК-1	способность выявлять возможные угрозы новых форм противоправной деятельности с применением информационно-коммуникационных и высоких технологий	ПСК-1.1.2	способность применять в профессиональной деятельности законодательство, регулирующее общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере, а также использовать современные информационно-коммуникационные и высокие технологии в противодействии транснациональной организованной преступности
ОПК ОС-5	способность внедрять новые технологии и методики противодействия угрозам национальной безопасности	ОПК ОС-5.1.6	способность принимать эффективные управленческие и правовые решения по противодействию угрозам национальной безопасности
ПК-9	способность выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения	ПК-9.3.2	способность соблюдать законодательство Российской Федерации в целях предотвращения коррупциогенных явлений, затрудняющих раскрытие преступления и иных правонарушений
ПК-10	способность применять в профессиональной деятельности теоретические основы раскрытия и расследования преступлений, использовать в целях установления объективной истины по конкретным делам технико-криминалистические методы и средства, тактические приемы производства следственных действий, формы организации и методику раскрытия и расследования отдельных	ПК-10.2.1	способность применять юридические технологии, криминалистическую технику и методику в деятельности по выявлению, пресечению, раскрытию и расследованию преступлений и иных правонарушений

	видов и групп преступлений		
ПК-11	способность реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	ПК-11.2.1	способность разрабатывать систему мер профилактики и предупреждения экономических и информационных угроз

Типовые оценочные средства

Вопросы для зачета:

1. Понятие информационной безопасности.
2. Место информационной безопасности в системе национальной безопасности.
3. Виды угроз информационной безопасности.
4. Источники угроз информационной безопасности Российской Федерации.
5. Система обеспечения информационной безопасности Российской Федерации.
6. Силы обеспечения информационной безопасности.
7. Средства обеспечения информационной безопасности.
8. Правовая база нормативно-правовых источников обеспечения информационной безопасности Российской Федерации.
9. Уголовно-правовая характеристика информационной безопасности.
10. Общая характеристика методов обеспечения информационной безопасности РФ.
11. Общие методы обеспечения информационной безопасности.
12. Понятие правовых методов обеспечения информационной безопасности.
13. Уголовно-правовые методы обеспечения информационной безопасности.
14. Организационно-технические методы обеспечения информационной безопасности.
15. Уголовно-правовая характеристика нарушения неприкосновенности частной жизни.
16. Объективные признаки нарушения неприкосновенности частной жизни.
17. Субъективные признаки нарушения неприкосновенности частной жизни.
18. Уголовно-правовая характеристика незаконного оборота специальных технических средств, предназначенных для негласного получения информации.
19. Объективные признаки незаконного оборота специальных технических средств, предназначенных для негласного получения информации.
20. Субъективные признаки незаконного оборота специальных технических средств, предназначенных для негласного получения информации.
21. Уголовно-правовая характеристика нарушения тайны переписки, телефонных

переговоров, почтовых, телеграфных или иных сообщений.

22. Объективные признаки нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

23. Субъективные признаки нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

24. Сведения, составляющие государственную, коммерческую или иную охраняемую законом тайну.

25. Уголовно-правовая характеристика преступных угроз безопасности охраняемой законом информации.

26. Уголовно-правовая характеристика разглашения государственной тайны.

27. Объективные признаки разглашения государственной тайны.

28. Субъективные признаки разглашения государственной тайны.

29. Уголовно-правовая характеристика утраты документов, содержащих государственную тайну.

30. Объективные признаки утраты документов, содержащих государственную тайну.

31. Субъективные признаки утраты документов, содержащих государственную тайну.

32. Уголовно-правовая характеристика преступных угроз информационной безопасности.

33. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.

34. Объективные признаки неправомерного доступа к компьютерной информации.

35. Субъективные признаки неправомерного доступа к компьютерной информации.

36. Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ.

37. Объективные признаки создания, использования и распространения вредоносных компьютерных программ.

38. Субъективные признаки создания, использования и распространения вредоносных компьютерных программ.

39. Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

40. Объективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

41. Субъективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

- 42. Формы уголовно-наказуемого информационного терроризма.
- 43. Уголовная ответственность за акт терроризма в форме угрозы совершения террористических действий.
- 44. Уголовно-правовая характеристика угрозы совершения террористических действий.
- 45. Объективные признаки угрозы совершения террористических действий.
- 46. Субъективные признаки угрозы совершения террористических действий.
- 47. Уголовная ответственность за заведомо ложное сообщение об акте терроризма.
- 48. Уголовно-правовая характеристика заведомо ложного сообщения об акте терроризма.
- 49. Объективные признаки заведомо ложного сообщения об акте терроризма.
- 50. Субъективные признаки заведомо ложного сообщения об акте терроризма.

Примерные варианты билетов к зачету

Билет № 1

1. Понятие информационной безопасности.
2. Уголовно-правовая характеристика разглашения государственной тайны.

Билет № 2

1. Место информационной безопасности в системе национальной безопасности.
2. Объективные признаки разглашения государственной тайны.

Билет № 3

1. Виды угроз информационной безопасности.
2. Субъективные признаки разглашения государственной тайны.

Билет № 4

1. Источники угроз информационной безопасности Российской Федерации.
2. Уголовно-правовая характеристика утраты документов, содержащих государственную тайну.

Билет № 5

1. Система обеспечения информационной безопасности Российской Федерации.
2. Объективные признаки утраты документов, содержащих государственную тайну.

Билет № 6

1. Силы обеспечения информационной безопасности.
2. Субъективные признаки утраты документов, содержащих государственную тайну.

Билет № 7

1. Средства обеспечения информационной безопасности.
2. Уголовно-правовая характеристика преступных угроз информационной безопасности.

Билет № 8

1. Правовая база нормативно-правовых источников обеспечения информационной безопасности Российской Федерации.
2. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.

Билет № 9

1. Уголовно-правовая характеристика информационной безопасности.
2. Объективные признаки неправомерного доступа к компьютерной информации.

Билет № 10

1. Общая характеристика методов обеспечения информационной безопасности РФ.
2. Субъективные признаки неправомерного доступа к компьютерной информации.

Билет № 11

1. Общие методы обеспечения информационной безопасности.
2. Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ.

Билет № 12

1. Понятие правовых методов обеспечения информационной безопасности.
2. Объективные признаки создания, использования и распространения вредоносных компьютерных программ.

Билет № 13

1. Уголовно-правовые методы обеспечения информационной безопасности.
2. Субъективные признаки создания, использования и распространения вредоносных компьютерных программ.

Билет № 14

1. Организационно-технические методы обеспечения информационной безопасности.
2. Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Билет № 15

1. Уголовно-правовая характеристика нарушения неприкосновенности частной жизни.
2. Объективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Шкала оценивания

Этап освоения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания
способность осуществлять анализ правотворческой деятельности органов власти, оценивать её соответствия государственной политике Российской Федерации в сфере развития и использования информационных технологий (УК ОС-2.1.5)	ориентация в правовых механизмах применения информационных технологий; анализ правотворческой деятельности органов власти в сфере развития и использования информационных технологий; оценка соответствия правотворческой деятельности государственной политике Российской Федерации в сфере развития и использования информационных технологий	уверено ориентируется в правовых механизмах применения информационных технологий; грамотно осуществляет анализ правотворческой деятельности органов власти в сфере развития и использования информационных технологий; самостоятельно осуществляет оценку соответствия правотворческой деятельности государственной политике Российской Федерации в сфере развития и использования информационных технологий	Опрос Кейсы-задания Тесты
способность применять в профессиональной деятельности законодательство, регулирующее общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере, а также использовать современные информационно-коммуникационные и высокие технологии в противодействии транснациональной организованной преступности (ПСК-1.1.2)	ориентируется в законодательстве, регулирующем общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере; применяются знания о современных информационно-коммуникационных и высоких технологиях в решении профессиональных ситуаций, связанных с противодействием транснациональной организованной преступности	уверено ориентируется в законодательстве, регулирующем общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере; грамотно и корректно применяет знания о современных информационно-коммуникационных и высоких технологиях в решении профессиональных ситуаций, связанных с выбором/предложениями по противодействию транснациональной организованной преступности	Опрос Кейсы-задания Тесты
способность принимать эффективные управленческие и правовые решения по противодействию угрозам национальной безопасности (ОПК ОС-5.1.6)	предложены организационные решения по противодействию угрозам национальной безопасности; сформулированы правовые решения по противодействию угрозам национальной безопасности; оценивается эффективность управленческих и правовых решений по противодействию угрозам национальной безопасности	грамотно определяет проблемы в сфере национальной безопасности с целью предложения организационных решений; аргументирует предложенные правовые и управленческие решения опираясь на конкретные законоположения и юридическую практику; оценивает и корректно описывает эффективность управленческих и правовых решения по противодействию угрозам национальной безопасности	Кейсы-задания
способность соблюдать законодательство Российской Федерации в	ориентируется в коррупционных явлениях, затрудняющих раскрытие	уверено ориентируется в коррупционных явлениях, затрудняющих раскрытие	Опрос Тесты Кейсы-задания

целях предотвращения коррупционных явлений, затрудняющих раскрытие преступлений и иных правонарушений (ПК-9.3.2)	преступления и иных правонарушений; – применяет положения законодательства Российской Федерации для выявления и профилактики коррупционного поведения и коррупционных явлений	преступления и иных правонарушений; – квалифицировано описывает и обосновывает положения, характеризующие коррупционные явления, обосновывает; приводит примеры действий по профилактике и борьбе с коррупционными явлениями	
способность применять юридические технологии, криминалистическую технику и методику в деятельности по выявлению, пресечению, раскрытию и расследованию преступлений и иных правонарушений (ПК-10.2.1)	– последовательно применяет научные основы, задачи и методы криминалистической идентификации на этапах пресечения, раскрытия и расследования преступлений и иных правонарушений; – применяются принципы организации раскрытия и расследования преступлений, криминалистическая тактика и методика	– умеет применять понятие, свойства и признаки объекта идентификационного комплекса, признаки идентификационного периода; – способен самостоятельно решать задачи криминалистической идентификации; – выделяет систему субъектов и объекты криминалистической идентификации, формы и виды криминалистической идентификации; – пользуется специальными криминалистическими методами: габитоскопии, документологии, оружейведения, дактилоскопии, трасологии, фотографии и др. приемами криминалистической техники; – соблюдение правовых основ применения технико-криминалистических средств и методов в деятельности по выявлению, пресечению, раскрытию и расследованию преступлений и иных правонарушений	Опрос Кейсы-задания
способность разрабатывать систему мер профилактики и предупреждения экономических и информационных угроз преступлений (ПК-11.2.1)	– выделяет ключевую и второстепенные задачи предупреждения, пресечения, раскрытия и расследования преступлений	– продемонстрировано глубокое понимание связи требований законодательства с использованием юридически значимой информации в интересах предупреждения, пресечения, раскрытия и расследования преступлений	Опрос Тесты Кейсы-задания

4.4. Методические материалы

Оценивание обучающихся в процессе поэтапного освоения ими компетенций, формируемых данной дисциплиной осуществляется в форме зачета, который предполагает оценивание *знаний* с помощью устного собеседования по узловым вопросам и *умений* решать ситуационные задачи и/или кейс-задания.

Знания и умения обучающегося на зачете оцениваются как «зачтено» или «не зачтено».

Оценивание обучающегося на зачете по дисциплине

Оценка	Критерии оценки	Результаты обучения
«зачтено»	<ul style="list-style-type: none"> – уверенно ориентируется в правовых механизмах применения информационных технологий; – грамотно осуществляет анализ правотворческой деятельности органов власти в сфере развития и использования информационных технологий; – самостоятельно осуществляет оценку соответствия правотворческой деятельности государственной политике Российской Федерации в сфере развития и использования информационных технологий; – уверенно ориентируется в законодательстве, регулирующее общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере; – грамотно и корректно применяет знания о современных информационно-коммуникационных и высоких технологиях в решении профессиональных ситуаций, связанных с выбором/предложениями по противодействию транснациональной организованной преступности; – грамотно определяет проблемы в сфере национальной безопасности с целью предложения организационных решений; – аргументирует предложенные правовые и управленческие решения опираясь на конкретные законоположения и юридическую практику; – оценивает и корректно описывает эффективность управленческих и правовых решения по противодействию угрозам национальной безопасности; – продемонстрировано глубокое понимание связи требований законодательства с использованием юридически значимой информации в интересах предупреждения, пресечения, раскрытия и расследования преступлений 	<p>УК ОС-2.1.5 на уровне знаний:</p> <ul style="list-style-type: none"> – пределов своей компетенции и основных компетенций взаимодействующих структур, практики и стереотипов принятия управленческих решений, планирования, документирования проектной деятельности; <p>на уровне умений:</p> <ul style="list-style-type: none"> – осуществлять исполнительскую, организационно-управленческую деятельность и нести за нее ответственность с позиций социальной значимости принимаемых решений в профессиональной сфере и соответствия их правовым и этическим нормам <p>ПСК-1.1.2 на уровне знаний:</p> <ul style="list-style-type: none"> – об основных положениях, их назначении и политико-правовой основе стратегии развития информационного общества в Российской Федерации <p>на уровне умений:</p> <ul style="list-style-type: none"> – применять в обеспечении информационной и национальной безопасности современные информационные, телекоммуникационные и иные высокие технологии <p>ОПК ОС-5.1.6 на уровне знаний:</p> <ul style="list-style-type: none"> – о видах угроз безопасности; – о последствиях реализации этих угроз; <p>на уровне умений:</p> <ul style="list-style-type: none"> – объективно оценивать влияние внешних и внутренних угроз на состояние национальной безопасности; – выделять ключевые факторы опасности и выстраивать приоритетность мер реагирования на них, применяя передовой отечественный и зарубежный опыт <p>ПК-9.3.2 на уровне знаний:</p> <ul style="list-style-type: none"> – особенностей предупреждений и профилактики отдельных видов правонарушений и преступлений; – положений и норм законодательства по
	– не знает правовые механизмы при-	

«не зачтено»	<p>менения информационных технологий;</p> <ul style="list-style-type: none"> – не способен анализировать право-творческую деятельность органов власти в сфере развития и использования информационных технологий; – не ориентируется в законодательстве, регулирующее общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере; – неправильно определяет проблемы в сфере национальной безопасности с целью предложения организационных решений; – демонстрирует непонимание связи требований законодательства с использованием юридически значимой информации в интересах предупреждения, пресечения, раскрытия и расследования преступлений 	<p>вопросам предупреждения и профилактики правонарушений и преступлений</p> <p>на уровне умений:</p> <ul style="list-style-type: none"> – соблюдать требования законности при выявлении и устранении причин и условий правонарушений и преступлений <p>ПК-10.2.1</p> <p>на уровне знаний:</p> <ul style="list-style-type: none"> – правовых и научных основ применения технико-криминалистических средств и методов выявления, пресечения, раскрытия и расследований преступлений и иных правонарушений <p>на уровне умений:</p> <ul style="list-style-type: none"> – применять научно обоснованные средства и методы криминалистической идентификации <p>ПК-11.2.1</p> <p>на уровне знаний:</p> <ul style="list-style-type: none"> – системы мер предупреждения, пресечения, раскрытия и расследования преступлений <p>на уровне умений:</p> <ul style="list-style-type: none"> – применять знания юридической техники в целях раскрытия, пресечения и профилактики правонарушений и преступлений
--------------	--	--

5. Методические указания для обучающихся по освоению дисциплины (модуля)

К зачету по дисциплине «Правовые основы борьбы с криминальными угрозами информационной безопасности» необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине.

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

- рабочей программой дисциплины;
- перечнем знаний, умений которыми обучающийся должен овладеть;
- тематическими планами занятий;
- контрольными мероприятиями;
- учебником, учебными пособиями, а также электронными ресурсами;
- перечнем вопросов к зачету и заданий.

После этого у обучающегося должно сформироваться четкое представление об объеме и характере знаний, умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение заданий учебной работы на лекциях и семинарских

занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

Промежуточная аттестация по дисциплине проводится в соответствии с Учебным планом по семестрам в 8 семестре для очной формы обучения в виде зачета.

Обучающийся допускается к зачету по дисциплине в случае выполнения им учебного плана. В случае наличия учебной задолженности обучающийся отрабатывает пропущенные занятия в форме, предложенной преподавателем.

Обучение по дисциплине предполагает контактную форму работы (лекционные, семинарские занятия) и самостоятельную работу обучающихся.

5.1. Методические рекомендации по подготовке к лекционным и семинарским занятиям

Изучение дисциплины содействует: приобретению студентами необходимой научно-теоретической базы и профессиональной подготовки по ключевым направлениям предупреждения криминальных угроз в сфере информационной безопасности Российской Федерации, формированию юридического мышления, знаний, умений и навыков применения положений и норм законодательства, иных нормативных правовых актов, регламентирующих предупредительную и профилактическую деятельность, высокого уровня правосознания, ориентации на неукоснительное соблюдение Конституции Российской Федерации, норм действующего законодательства РФ и международного права по вопросам борьбы с преступностью и предупреждению преступлений в сфере информации. В связи с этим 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 предполагается задать лектору по проблеме предстоящей лекции.

Цель семинарских занятий заключается в умении применять полученные знания в практической деятельности; в более глубоком осмыслении механизмов правового регулирования; в формировании гражданского мировоззрения на основе знаний принципов правосудия, нормативно-правовых актов.

Вопросы для самостоятельной подготовки к семинарским занятиям

Семинар № 1. Понятие и место информационной безопасности в системе национальной безопасности России

1. Понятие информационной безопасности.
2. Место информационной безопасности в системе национальной безопасности.
3. Виды угроз информационной безопасности.
4. Источники угроз информационной безопасности Российской Федерации.
5. Система обеспечения информационной безопасности Российской Федерации.
6. Силы обеспечения информационной безопасности.
7. Средства обеспечения информационной безопасности.
8. Правовая база нормативно-правовых источников обеспечения информационной безопасности Российской Федерации.

Семинар № 2. Информационная безопасность как объект уголовно-правовой защиты

1. Уголовно-правовая характеристика информационной безопасности.
 2. Общая характеристика методов обеспечения информационной безопасности РФ.
 3. Общие методы обеспечения информационной безопасности.
 4. Понятие правовых методов обеспечения информационной безопасности.
 5. Уголовно-правовые методы обеспечения информационной безопасности.
- Организационно-технические методы обеспечения информационной безопасности.

Семинар № 3. Уголовно-правовые меры защиты информационной безопасности личности

1. Уголовно-правовая характеристика нарушения неприкосновенности частной жизни.
2. Объективные признаки нарушения неприкосновенности частной жизни.
3. Субъективные признаки нарушения неприкосновенности частной жизни.
4. Уголовно-правовая характеристика незаконного оборота специальных технических средств, предназначенных для негласного получения информации.
5. Объективные признаки незаконного оборота специальных технических средств, предназначенных для негласного получения информации.
6. Субъективные признаки незаконного оборота специальных технических средств, предназначенных для негласного получения информации.
7. Уголовно-правовая характеристика нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
8. Объективные признаки нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
9. Субъективные признаки нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Семинар № 4. Уголовно-правовые меры защиты от криминальных угроз безопасности охраняемой законом информации

1. Сведения, составляющие государственную, коммерческую или иную охраняемую законом тайну.
2. Уголовно-правовая характеристика преступных угроз безопасности охраняемой законом информации.
3. Уголовно-правовая характеристика разглашения государственной тайны.
4. Объективные признаки разглашения государственной тайны.
5. Субъективные признаки разглашения государственной тайны.
6. Уголовно-правовая характеристика утраты документов, содержащих государственную тайну.
7. Объективные признаки утраты документов, содержащих государственную тайну.
8. Субъективные признаки утраты документов, содержащих государственную тайну.

тайну.

Семинар № 5. Уголовно-правовые меры защиты безопасности в сфере высоких информационных технологий

1. Уголовно-правовая характеристика преступных угроз информационной безопасности.
2. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.
3. Объективные признаки неправомерного доступа к компьютерной информации.
4. Субъективные признаки неправомерного доступа к компьютерной информации.
5. Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ.
6. Объективные признаки создания, использования и распространения вредоносных компьютерных программ.
7. Субъективные признаки создания, использования и распространения вредоносных компьютерных программ.
8. Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
9. Объективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
10. Субъективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Семинар № 6. Уголовно-правовые меры защиты от угроз информационного терроризма

1. Формы уголовно-наказуемого информационного терроризма.
2. Уголовно-правовая характеристика угрозы совершения террористических действий.
3. Объективные признаки угрозы совершения террористических действий.
4. Субъективные признаки угрозы совершения террористических действий.
5. Уголовная ответственность за заведомо ложное сообщение об акте терроризма.
6. Уголовно-правовая характеристика заведомо ложного сообщения об акте терроризма.
7. Объективные признаки заведомо ложного сообщения об акте терроризма.
8. Субъективные признаки заведомо ложного сообщения об акте терроризма.

5.2. Методические рекомендации к самостоятельной работе

Основной целью самостоятельной работы студентов является улучшение юридической профессиональной подготовки специалистов, направленное на формирование системы фундаментальных и профессиональных знаний, умений и навыков, которые они могли бы свободно и самостоятельно применять в практической деятельности.

Самостоятельная работа обучающихся направлена на решение следующих задач – углублять, расширять юридические профессиональные знания специалистов и формировать у них интерес к учебно-познавательной деятельности в сфере изучения правоохранительных органов, их структуры и деятельности:

- углублять, расширять профессиональные знания студентов и формировать у них интерес к учебно-познавательной деятельности;
- научить студентов овладевать приемами анализа криминогенной ситуации, причин и условий преступности и других криминальных угроз в сфере обеспечения приоритетов национальной безопасности Российской Федерации;
- развивать у них самостоятельность, активность, ответственность в ходе изучения учебной дисциплины;
- развивать познавательные способности будущих юристов по овладению профессиональной компетенцией.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия. Для обеспечения внеаудиторной самостоятельной работы по дисциплине преподавателем разрабатывается перечень заданий для самостоятельной работы, который необходим для эффективного управления данным видом учебной деятельности обучающихся. Самостоятельная работа студентов включает подготовку к устному опросу. Для этого студент изучает лекции, основную и дополнительную литературу, публикации, информацию из Интернет-ресурсов, и электронных библиотечных баз. Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня подготовленности обучающихся. Обучающийся самостоятельно определяет режим своей внеаудиторной работы и меру труда, затрачиваемого на овладение знаниями и умениями по дисциплине, выполняет внеаудиторную работу по индивидуальному плану, в зависимости от собственной подготовки, бюджета времени и других условий. Ежедневно обучающийся должен уделять выполнению внеаудиторной самостоятельной работы в среднем не менее 3 часов. При выполнении внеаудиторной самостоятельной работы обучающийся имеет право обращаться к преподавателю за консультацией с целью уточнения задания, формы контроля выполненного задания. Эффективность подготовки студентов зависит от качества ознакомления с рекомендованной литературой. Для подготовки к устному

опросу студенту необходимо ознакомиться с материалом, посвященным изучаемой теме в учебнике или другой рекомендованной литературе, записях с лекционного занятия. Развернутый ответ должен следовать определенной логике и последовательности изложения, состоять из многих предложений, содержать доводы и выводы.

5.3. Методические рекомендации для подготовки к опросам по вынесенным на обсуждение темам

Устные опросы проводятся во время семинарских/практических занятий и возможны при проведении зачета в качестве дополнительного испытания при недостаточности результатов тестирования и решения заданий. Вопросы опроса не должны выходить за рамки объявленной для данного занятия темы. Устные опросы необходимо строить так, чтобы вовлечь в тему обсуждения максимальное количество обучающихся в группе, проводить параллели с уже пройденным учебным материалом данной дисциплины и смежными курсами, находить удачные примеры из современной действительности, что увеличивает эффективность усвоения материала на ассоциациях. Основные вопросы для устного опроса доводятся до сведения студентов на предыдущем практическом занятии. Письменные опросы позволяют проверить уровень подготовки к практическому занятию всех обучающихся в группе, при этом оставляя достаточно учебного времени для иных форм педагогической деятельности в рамках данного занятия. Письменный опрос проводится без предупреждения, что стимулирует обучающихся к систематической подготовке к занятиям. Вопросы для опроса готовятся заранее, формулируются узко, дабы обучающийся имел объективную возможность полноценно его осветить за отведенное время (10 – 15 мин.). Письменные опросы целесообразно применять в целях проверки усвояемости значительного объема учебного материала, например, во время проведения экзамена, когда необходимо проверить знания студентов по всему курсу. При оценке опросов анализу подлежит точность формулировок, связность изложения материала, обоснованность суждений, опора на действующее семейное законодательство.

5.4. Методические рекомендации по решению ситуационных задач и кейс-заданий

Кейс-задание (case) – это конкретная практическая ситуация, рассказывающая о той или иной ситуации, в которой зачастую заложена некая проблема.

Выполнение кейс-заданий осуществляется с целью проверки уровня навыков (владений) студента по применению норм права, по правильному толкованию норм закона, быстрому и эффективному ориентированию в системе норм законодательства, по решению вопросов в области отдельных правоотношений. Студенту объявляется условие задания, решение которого он излагает устно. Эффективным интерактивным

способом решения задания является сопоставления результатов разрешения одного задания двумя и более малыми группами обучающихся. Задачи, требующие изучения значительного объема нормативного или правоприменительного материала, необходимо относить на самостоятельную работу студентов, с непременно разбором результатов во время практических занятий. В данном случае решение ситуационных задач с глубоким обоснованием должно представляться на проверку в письменном виде. При оценке решения заданий анализируется понимание студентом конкретной ситуации, правильность применения норм права, способность обоснования выбранной точки зрения, глубина проработки правоприменительного материала, умением выявить основные положения нормативного документа.

5.5. Методические рекомендации по выполнению тестовых заданий

Тестирование проводится 1 раз в течение семестра. Не менее чем за 1 неделю до тестирования, преподаватель должен определить студентам исходные данные для подготовки к тестированию: назвать разделы (темы, вопросы), по которым будут задания в тестовой форме, нормативные правовые акты и теоретические источники (с точным указанием разделов, тем, статей) для подготовки. При прохождении тестирования пользоваться конспектами лекций, учебниками, и нормативными актами не разрешено.

Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступить к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать лишь один индекс (цифровое обозначение), соответствующий правильному ответу, если нет специальной оговорки, что может быть несколько правильных ответов.

Тесты составлены таким образом, что в каждом из них правильным является как один, так и несколько вариантов. Выбор должен быть сделан в пользу наиболее правильного или правильных ответов.

На выполнение теста отводится ограниченное время. Оно может варьироваться в зависимости от уровня тестируемых, сложности и объема теста.

Критерии оценки выполненных студентами тестов определяются преподавателем самостоятельно. Рекомендуются следующие критерии оценки:

- 85% – 100% правильных ответов – «отлично»;
- 66% – 84% правильных ответов – «хорошо»;
- 50% – 65% правильных ответов – «удовлетворительно»;
- менее 50% правильных ответов – «неудовлетворительно».

При подведении итогов по выполненной работе рекомендуется проанализировать допущенные ошибки, прокомментировать имеющиеся в тестах неправильные ответы.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Основная литература

1. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс]: учебник для магистров и аспирантов/ А.В. Морозов, Л.В. Филатова, Т.А. Полякова— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 604 с.— Режим доступа: <http://www.iprbookshop.ru/66771.html>.— ЭБС «IPRbooks».
2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ С.В. Петров, П.А. Кисляков— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: <http://www.iprbookshop.ru/33857.html>.— ЭБС «IPRbooks».

6.2. Дополнительная литература

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/33430.html>.— ЭБС «IPRbooks».
2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В. Прохорова— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183.html>.— ЭБС «IPRbooks».
3. Зеленков М.Ю. Основы теории национальной безопасности [Электронный ресурс]: учебник для студентов вузов / Зеленков М.Ю. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2016. 296 с. Режим доступа: <http://www.iprbookshop.ru/54282.html>. ЭБС «IPRbooks».
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: <http://www.iprbookshop.ru/63594.html>.— ЭБС «IPRbooks».

6.3. Учебно-методическое обеспечение самостоятельной работы

Тема 1. Понятие и место информационной безопасности в системе национальной безопасности России

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и

выживания (МАБИВ), 2014.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/33430.html>.— ЭБС «IPRbooks».

2. Зеленков М.Ю. Основы теории национальной безопасности [Электронный ресурс]: учебник для студентов вузов / Зеленков М.Ю. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2016. 296 с. Режим доступа: <http://www.iprbookshop.ru/54282.html>. ЭБС «IPRbooks».

3. Плетников В.С. Обеспечение общественной безопасности (теоретико-прикладные аспекты) [Электронный ресурс]: монография / Плетников В.С., Федоров А.Ю., Плетникова М.С. Электрон. текстовые данные. Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2012. 87 с. Режим доступа: <http://www.iprbookshop.ru/26255.html>. ЭБС «IPRbooks».

4. Правовая основа обеспечения национальной безопасности Российской Федерации [Электронный ресурс]: монография / Л.Н. Башкатов [и др.]. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2012. 512 с. Режим доступа: <http://www.iprbookshop.ru/8752.html>. ЭБС «IPRbooks».

5. Чернявская Н.М. Основы национальной безопасности [Электронный ресурс]: учебное пособие / Чернявская Н.М. Электрон. текстовые данные. Комсомольск-на-Амуре: Амурский гуманитарно-педагогический государственный университет, 2011. 293 с. Режим доступа: <http://www.iprbookshop.ru/22279.html>. ЭБС «IPRbooks».

Тема 2. Информационная безопасность как объект уголовно-правовой защиты

1. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В. Прохорова— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183.html>.— ЭБС «IPRbooks».

2. Дьяков С.В. Преступления против основ конституционного строя и безопасности государства. Уголовно-правовое и криминологическое исследование [Электронный ресурс]: монография / Дьяков С.В. Электрон. текстовые данные. СПб.: Юридический центр Пресс, 2012. 267 с. Режим доступа: <http://www.iprbookshop.ru/9260.html>. ЭБС «IPRbooks».

3. Кибальчик А.Г. Преступления против мира и безопасности человечества [Электронный ресурс] / Кибальчик А.Г., Соломоненко И.Г. Электрон. текстовые данные. СПб.: Юридический центр Пресс, 2004. 385 с. Режим доступа: <http://www.iprbookshop.ru/18036.html>. ЭБС «IPRbooks».

4. Наумова Ю.Н. Особенности расследования преступлений, предусмотренных международными договорами Российской Федерации [Электронный ресурс]: учебное пособие / Наумова Ю.Н. Электрон. текстовые данные. М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014. 117 с. Режим доступа: <http://www.iprbookshop.ru/47249.html>. ЭБС «IPRbooks».

5. Савицкий А.Г. Национальная безопасность. Россия в мире [Электронный ресурс]: учебник / Савицкий А.Г. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2012. 463 с. Режим доступа: <http://www.iprbookshop.ru/15422.html>. ЭБС «IPRbooks».

Тема 3. Уголовно-правовые меры защиты информационной безопасности личности

1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие / С.В. Петров, П.А. Кисляков— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: <http://www.iprbookshop.ru/33857.html>.— ЭБС «IPRbooks».
2. Зеленков М.Ю. Основы теории национальной безопасности [Электронный ресурс]: учебник для студентов вузов / Зеленков М.Ю. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2016. 296 с. Режим доступа: <http://www.iprbookshop.ru/54282.html>. ЭБС «IPRbooks».
3. Кардашова И.Б. Обеспечение национальной безопасности [Электронный ресурс]: учебное пособие / Кардашова И.Б. Электрон. текстовые данные. М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2015. 136 с. Режим доступа: <http://www.iprbookshop.ru/43226.html>. ЭБС «IPRbooks».
4. Плетников В.С. Обеспечение общественной безопасности (теоретико-прикладные аспекты) [Электронный ресурс]: монография / Плетников В.С., Федоров А.Ю., Плетникова М.С. Электрон. текстовые данные. Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2012. 87 с. Режим доступа: <http://www.iprbookshop.ru/26255.html>. ЭБС «IPRbooks».
5. Структура системы обеспечения безопасности Российской Федерации [Электронный ресурс]: учебное пособие / В.И. Аверченков [и др.]. Электрон. текстовые данные. Брянск: Брянский государственный технический университет, 2012. 140 с. Режим доступа: <http://www.iprbookshop.ru/7011.html>. ЭБС «IPRbooks».

Тема 4. Уголовно-правовые меры защиты от криминальных угроз безопасности охраняемой законом информации

1. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. Прохорова— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183.html>.— ЭБС «IPRbooks».
2. Братановский С.Н. Прокуратура Российской Федерации в механизме защиты конституционных прав и свобод человека и гражданина [Электронный ресурс]: монография / Братановский С.Н., Урываев А.В. Электрон. текстовые данные. Саратов: Электронно-библиотечная система IPRbooks, 2012. 244 с. Режим доступа: <http://www.iprbookshop.ru/9011.html>. ЭБС «IPRbooks».
3. Кардашова И.Б. Система национальной безопасности Российской Федерации [Электронный ресурс]: учебное пособие / Кардашова И.Б. Электрон. текстовые данные. М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014. 142 с. Режим доступа: <http://www.iprbookshop.ru/42506.html>. ЭБС «IPRbooks».
4. Обеспечение прав и свобод человека правоохранительными органами Российской Федерации [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по специальности «Юриспруденция» / В.Я. Кикоть [и др.]. Электрон. текстовые данные. М.:

ЮНИТИ-ДАНА, 2012. 319 с. Режим доступа: <http://www.iprbookshop.ru/8771.html>. ЭБС «IPRbooks».

5. Плетников В.С. Обеспечение общественной безопасности (теоретико-прикладные аспекты) [Электронный ресурс]: монография / Плетников В.С., Федоров А.Ю., Плетникова М.С. Электрон. текстовые данные. Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2012. 87 с. Режим доступа: <http://www.iprbookshop.ru/26255.html>. ЭБС «IPRbooks».

6. Правовая основа обеспечения национальной безопасности Российской Федерации [Электронный ресурс]: монография / Л.Н. Башкатов [и др.]. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2012. 512 с. Режим доступа: <http://www.iprbookshop.ru/8752.html>. ЭБС «IPRbooks».

7. Структура системы обеспечения безопасности Российской Федерации [Электронный ресурс]: учебное пособие / В.И. Аверченков [и др.]. Электрон. текстовые данные. Брянск: Брянский государственный технический университет, 2012. 140 с. Режим доступа: <http://www.iprbookshop.ru/7011.html>. ЭБС «IPRbooks».

Тема 5. Уголовно-правовые меры защиты безопасности в сфере высоких информационных технологий

1. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс]: учебник для магистров и аспирантов/ А.В. Морозов, Л.В. Филатова, Т.А. Полякова— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 604 с.— Режим доступа: <http://www.iprbookshop.ru/66771.html>.— ЭБС «IPRbooks».

2. Зубков В.А. Международные стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризма [Электронный ресурс]: учебное пособие / Зубков В.А., Осипов С.К. Электрон. текстовые данные. М.: Юриспруденция, 2012. 367 с. Режим доступа: <http://www.iprbookshop.ru/8075.html>. ЭБС «IPRbooks».

3. Кибальчик А.Г. Преступления против мира и безопасности человечества [Электронный ресурс] / Кибальчик А.Г., Соломоненко И.Г. Электрон. текстовые данные. СПб.: Юридический центр Пресс, 2004. 385 с. Режим доступа: <http://www.iprbookshop.ru/18036.html>. ЭБС «IPRbooks».

4. Килясханов Х.Ш. ОБСЕ в борьбе с терроризмом [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по специальности «Юриспруденция» / Килясханов Х.Ш., Гончаров И.В. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2013. 523 с. Режим доступа: <http://www.iprbookshop.ru/20981.html>. ЭБС «IPRbooks».

5. Противодействие преступлениям террористической и экстремистской направленности. Вопросы теории и практики оперативно-розыскной деятельности [Электронный ресурс]: учебно-методическое пособие для студентов, обучающихся по специальности «Юриспруденция» / В.В. Волченков [и др.]. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2015. 431 с. Режим доступа: <http://www.iprbookshop.ru/52544.html>.— ЭБС «IPRbooks».

6. Терроризм и организованная преступность [Электронный ресурс]: монография / Н.Д. Эриашвили [и др.]. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2012. 247 с. Режим доступа: <http://www.iprbookshop.ru/8784.html>. ЭБС «IPRbooks».

Тема 6. Уголовно-правовые меры защиты от угроз информационного терроризма

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/33430.html>.— ЭБС «IPRbooks».

2. Ломакин В.В. Совершенствование деятельности органов государственной власти по противодействию экстремизму в Российской Федерации [Электронный ресурс]: монография / Ломакин В.В., Карпов А.В. Электрон. текстовые данные. М.: Дашков и К, 2015. 115 с. Режим доступа: <http://www.iprbookshop.ru/60321.html>. ЭБС «IPRbooks».

3. Противодействие преступлениям террористической и экстремистской направленности. Вопросы теории и практики оперативно-розыскной деятельности [Электронный ресурс]: учебно-методическое пособие для студентов, обучающихся по специальности «Юриспруденция» / В.В. Волченков [и др.]. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2015. 431 с. Режим доступа: <http://www.iprbookshop.ru/52544.html>.— ЭБС «IPRbooks».

4. Тамаев Р.С. Уголовно-правовое и криминологическое обеспечение противодействия экстремизму [Электронный ресурс]: монография / Тамаев Р.С. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2012. 279 с. Режим доступа: <http://www.iprbookshop.ru/8785.html>. ЭБС «IPRbooks».

5. Тамаев Р.С. Экстремизм и национальная безопасность. Правовые проблемы [Электронный ресурс]: монография / Тамаев Р.С. Электрон. текстовые данные. М.: ЮНИТИ-ДАНА, 2012. 263 с. Режим доступа: <http://www.iprbookshop.ru/8791.html>. ЭБС «IPRbooks».

6. Экстремизм и его причины // [Электронный ресурс]: монография / Ю.М. Антонян [и др.]. Электрон. текстовые данные. М.: Логос, 2013. 312 с. Режим доступа: <http://www.iprbookshop.ru/9129.html>. ЭБС «IPRbooks».

6.4. Нормативные правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993), (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства Российской Федерации. 04.08.2014. № 31. Ст. 4398.

2. Федеральный конституционный закон от 31.12.1996 № 1-ФКЗ (ред. от 05.02.2014) «О судебной системе Российской Федерации» // Собрание законодательства Российской Федерации. 06.01.1997. № 1. Ст. 1.

3. Федеральный закон от 17 января 1992 г. № 2202-1 «О прокуратуре Российской

Федерации» (с изменениями и дополнениями, вступившими в силу с 15.09.2015) // Собрание законодательства Российской Федерации. 20.11.1995. № 47. Ст. 4472.

4. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» (ред. от 22.12.2014) // Собрание законодательства Российской Федерации. 10.04.1995. № 15. Ст. 1269.

5. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.06.2015) «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. 14.08.1995. № 33. Ст. 3349.

6. Федеральный закон от 10.01.1996 № 5-ФЗ (ред. от 23.06.2014) «О внешней разведке» // Собрание законодательства Российской Федерации. 15.01.1996. № 3. Ст. 143.

7. Федеральный закон от 27 мая 1996 г. № 57-ФЗ (ред. от 12.03.2014) «О государственной охране» // Собрание законодательства Российской Федерации. 27.05.1996. № 22. Ст. 2594.

8. Федеральный закон от 21.07.1997 № 114-ФЗ (ред. от 22.12.2014) «О службе в таможенных органах Российской Федерации» // Собрание законодательства Российской Федерации. 28.07.1997. № 30. Ст. 3586.

9. Федеральный закон от 07 августа 2001 г. № 115-ФЗ (ред. от 29.06.2015) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства Российской Федерации. 13.08.2001. № 33. Ст. 3418.

10. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 08.03.2015) «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации. 29.07.2002. № 30. Ст. 3031.

11. Федеральный закон от 06 марта 2006 г. № 35-ФЗ (ред. от 31.12.2014) «О противодействии терроризму» // Собрание законодательства Российской Федерации. 13.03.2006. № 11. Ст. 1146.

12. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // Собрание законодательства Российской Федерации. 03.01.2011. № 1. Ст. 2.

13. Федеральный закон от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации» (с изменениями и дополнениями, вступившими в силу с 03.01.2015) // Собрание законодательства Российской Федерации. 03.01.2011. № 1. Ст. 15.

14. Федеральный закон от 07 февраля 2011 г. № 3-ФЗ «О полиции» (с изменениями и дополнениями, вступившими в силу с 15.09.2015) // Собрание законодательства Российской Федерации. 14.02.2011. № 7. Ст. 900.

15. Указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Собрание законодательства Российской Федерации. 18.05.2009. № 20. Ст. 2444.

16. Указ Президента РФ от 06.05.2011 № 590 (ред. от 25.07.2014) «Вопросы Совета Безопасности Российской Федерации» (вместе с «Положением о Совете Безопасности

Российской Федерации», «Положением об аппарате Совета Безопасности Российской Федерации», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по безопасности в экономической и социальной сфере», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по военной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по общественной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по проблемам Содружества Независимых Государств», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по проблемам стратегического планирования», «Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по экологической безопасности», «Положением о научном совете при Совете Безопасности Российской Федерации») // Собрание законодательства Российской Федерации. 09.05.2011. № 19. Ст. 2721.

17. Указ Президента РФ от 19.12.2012 № 1666 «О Стратегии государственной национальной политики Российской Федерации на период до 2025 года» // Собрание законодательства Российской Федерации. 24.12.2012. № 52. Ст. 7477.

18. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. № 187. 28.09.2000.

19. Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу (утв. Президентом РФ 18.09.2008 № Пр-1969) // Справочно-правовая система «Гарант».

6.5. Интернет-ресурсы

1. www.kremlin.ru – Президент Российской Федерации
2. www.gov.ru – Сервер органов государственной власти Российской Федерации
3. <http://www.gov.ru/main/page7.html> – Федеральное собрание РФ
4. <http://www.duma.gov.ru/> – Государственная Дума ФС РФ
5. www.vsrf.ru – Верховный Суд Российской Федерации
6. www.ksrf.ru – Конституционный Суд Российской Федерации

6.6. Базы данных, информационно-справочные и поисковые системы

1. www.consultant.ru – Справочная правовая система «КонсультантПлюс»
2. СПС Гарант v.7 – Справочно-Правовая Система
3. <http://diss.rsl.ru> – Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ. Включает полнотекстовые базы данных

диссертаций.

4. www.iqlib.ru – Электронная библиотека образовательных и научных изданий.
5. <http://www.cir.ru> – Университетская информационная система «Россия».
6. www.public.ru – Интернет-библиотека СМИ.

6.7. Иные источники

1. Авдеев В.А., Авдеева О.А. Механизм противодействия преступлениям террористического характера и экстремистской направленности в Российской Федерации // Юридический мир. 2014. № 12. С. 59 – 63.
2. Борщ А.А. Национальная безопасность и власть. РАНХиГС при Президенте РФ, Факультет национальной безопасности. М., 2012.
3. Босхамджиева Н.А. Административно-правовые основы обеспечения общественной безопасности в Российской Федерации. М., 2014.
4. Глобальная безопасность: инновационные методы анализа конфликтов Под общ. ред. А. И. Смирнова. М., 2011.
5. Голованова Н.А. Экстремизм в Великобритании: способы противодействия // Журнал российского права. 2014. № 4. С. 102 – 111.
6. Зубков В.А., Осипов С.К. Международные стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризма: учебное пособие. М., 2010.
7. Кабасакалова М.Г. Российско-американское сотрудничество в сфере борьбы с международным терроризмом // Международное публичное и частное право. 2014. № 3. С. 21 – 24.
8. Кафтан В.В. Противодействие терроризму. Учебное пособие для бакалавриата и магистратуры. М., 2015.
9. Медов М.У. Основные причины распространения терроризма // Российский следователь. 2015. № 8. С. 38 – 42.
10. Меркурьев В.В. Террористические преступления в новой редакции Уголовного кодекса // Законы России: опыт, анализ, практика. 2013. № 10. С. 47 – 56.
11. Мохов Е.А. Организованная преступность и национальная безопасность России: монография. М.: Вузовская книга, 2002.
12. Обеспечение национальной безопасности России: библиографический указатель. Управление информационного и документационного обеспечения Президента Российской Федерации, Департамент по обеспечению деятельности Библиотеки Администрации Президента Российской Федерации. М., 2012.
13. Паненков А.А. Борьба с финансированием терроризма (российский и зарубежный опыт) // Международное уголовное право и международная юстиция. 2013. № 6. С. 10 – 14.
14. Солодовников С.А. Терроризм и организованная преступность. М., 2013.
15. Сухаренко А.Н. Российская организованная преступность в Евросоюзе: состояние и меры борьбы // Международное уголовное право и международная юстиция. 2013. № 1. С. 3 – 5.

16. Чапчиков С.Ю. Необходима конституционная доктрина безопасности личности, общества, государства // Конституционное и муниципальное право. 2011. № 6. С. 14 – 18.

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).

5. Информационные справочные и поисковые системы «Консультант Плюс», «Гарант».