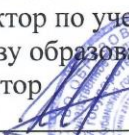


Министерство образования и науки Российской Федерации  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Кубанский государственный университет»  
Юридический факультет имени А.А. Хмырова

УТВЕРЖДАЮ:  
Проректор по учебной работе,  
качеству образования — первый  
проректор  
  
Хагуров Т.А.  
« 27 » апреля 2018 г.



### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

#### **Б1.В.ДВ.06.02 ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Специальность 40.05.01 «Правовое обеспечение национальной безопасности»

Специализация: уголовно-правовая

Форма обучения: очная

Квалификация (степень) выпускника: юрист

Краснодар 2018

Рабочая программа дисциплины «Преступления против информационной безопасности» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 40.05.01 «Правовое обеспечение национальной безопасности» (уровень специалитета), утвержденным приказом Минобрнауки России от 19 декабря 2016 г. N 1614.

Программу составил:

**Грошев А.В.**, д.ю.н., проф.   
\_\_\_\_\_  
фамилия, инициалы, подпись

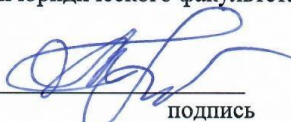
Рабочая программа дисциплины «Преступления против информационной безопасности» утверждена на заседании кафедры уголовного права и криминологии, протокол № 18 «13» апреля 2018 г.

Заведующий кафедрой уголовного права  
и криминологии                      Коняхин В.П.

  
\_\_\_\_\_  
подпись

Утверждена на заседании учебно-методической комиссии юридического факультета, протокол № 10 «16» апреля 2018 г.

Председатель УМК факультета    Прохорова М.Л.

  
\_\_\_\_\_  
подпись

Рецензенты:

Медведев С.С., доцент кафедры уголовного права Кубанского государственного аграрного университета, к.ю.н., доц.,

Тушев А.А., зам. декана по учебной работе юридического факультета Кубанского государственного аграрного университета, д.ю.н., проф.

## **1 Цели и задачи изучения дисциплины**

### **1.1 Цель дисциплины**

Учебная дисциплина «Преступления против информационной безопасности» имеет своей целью формирование у студентов общекультурных и профессиональных компетенций, необходимых для последующей успешной реализации правовых норм, обеспечения законности и правопорядка, правового обучения и воспитания.

Цель преподавания дисциплины «Преступления против информационной безопасности» - формирование на основе положений теории уголовного права целостного представления о системе преступлений в сфере компьютерной информации, их уголовно-правовом содержании и основных направлениях борьбы с ними; практических навыков и умений самостоятельного применения уголовного закона, регламентирующего ответственность за преступления в сфере компьютерной информации на практике в соответствии с требованиями, установленными Государственным образовательным стандартом высшего профессионального образования по направлению «Юриспруденция».

Предмет изучения дисциплины - изучение специфики квалификации компьютерных преступлений, особенностей разграничения смежных составов преступлений и отграничения преступлений от иных правонарушений.

### **1.2 Задачи дисциплины**

Основными *задачами* изучения названной учебной дисциплины выступают:

- анализ системы преступлений в сфере компьютерной информации и их криминологическая характеристика;
- изучение нормативного материала, необходимого для усвоения содержания составов преступлений; в сфере компьютерной информации;
- изучение вопросов квалификации названных преступлений и практики применения соответствующих норм УК РФ;
- сравнительно-правовой анализ преступлений в сфере компьютерной информации в российском и зарубежном уголовном законодательстве.
- ознакомление с основными направлениями борьбы с преступлениями в сфере компьютерной информации.

Освоение дисциплины направлено на формирование у студентов способности работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; способность юридически правильно квалифицировать факты, события и обстоятельства; способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности; способность правильно и точно квалифицировать факты, события и обстоятельства, связанные с совершением преступлений против национальной безопасности.

### 1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Преступления против информационной безопасности» относится к вариативной части профессионального цикла Блока 1 «Дисциплины» учебного плана, выступая в качестве дисциплины по выбору (Б1.В.ДВ.06.02).

Курс дисциплины «Преступления против информационной безопасности» занимает важное место в процессе воспитания правового сознания и правовой культуры студентов, и служит надёжной основой для дальнейшего освоения правовых дисциплин.

Успешное освоение дисциплины «Преступления против информационной безопасности» создаст прочный базис для принятия решений в точном соответствии с законом, правильной квалификации фактов и обстоятельств, обеспечения соблюдения законодательства субъектами права, послужит основой для дальнейшей научно-исследовательской и практической деятельности.

*Требования к предварительной подготовке обучающегося:*

Для успешного освоения дисциплины студент должен иметь базовую подготовку по следующим дисциплинам – теория и история государства и права, конституционное право, административное право, уголовное право, международное уголовное право, зарубежное уголовное право, информационное право, административное право криминология, квалификация преступлений, получаемую в процессе обучения на предыдущих курсах или при параллельном освоении соответствующей материи.

*Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:*

Дисциплина «Преступления против информационной безопасности» является базовой для успешного прохождения и освоения практик, формирующих профессиональные навыки обучающихся, прохождения государственной итоговой аттестации, написания и защиты выпускной квалификационной работы, а также для последующего успешного обучения в магистратуре и аспирантуре.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных, профессиональных и профессиональщ - специализированных компетенций (ОПК, ПК и ПСК):

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-12	способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства	основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, информационные ресурсы и технологии, в том числе	работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска,	навыками работы с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска,

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		получения, хранения, поиска, систематизации, обработки и передачи информации	применительно к институту ответственности за преступления против информационной безопасности.	систематизации, обработки и передачи информации, в том числе применительно к институту ответственности за преступления против информационной безопасности.	систематизации, обработки и передачи информации в своей профессиональной деятельности, в том числе применительно к институту ответственности за преступления против информационной безопасности.
2.	ПК-2	способность юридически правильно квалифицировать факты, события и обстоятельства	содержание и основные правила юридической квалификации фактов, событий и обстоятельств, в том числе связанных с совершением преступлений против информационной безопасности..	выявлять факты и обстоятельства, в том числе связанные с совершением преступления против информационной безопасности, требующие правовой квалификации, правильно определять круг нормативно-правовых актов, нормы которых распространяются на данные факты и обстоятельства, давать юридическую оценку сложившейся ситуации	навыками юридического анализа правоотношений, являющихся объектами профессиональной деятельности, квалификации фактов, событий и обстоятельств, в том числе связанных с совершением преступления против информационной безопасности., и их уголовно-правовой оценки (квалификации)
3.	ПК-16	способность соблюдать в профессиональной деятельности требования	требования нормативных правовых актов в области защиты государственной тайны и	правильно определять подлежащие применению в профессиональной деятельности	навыками применения в профессиональной деятельности требований нормативных

№ п.п.	Индекс компет енции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	информационной безопасности, способы соблюдение и обеспечения режима секретности, в том числе при анализе и квалификации. преступления против информационной безопасности.	нормативные акты в области защиты государственной тайны и информационной безопасности, обеспечения соблюдения режима секретности, в том числе при квалификации преступления против информационной безопасности.	правовых актов в области защиты государственной тайны и информационной безопасности, обеспечения режима секретности, в том числе при анализе и квалификации преступления против информационной безопасности.
	ПСК-4	способность правильно и точно квалифицировать факты, события и обстоятельств, связанные с совершением преступлений против основ национальной безопасности	содержание и основные правила юридической квалификации юридических фактов и связанных с ними обстоятельств, при анализе преступлений против основ национальной безопасности, в том числе при квалификации . преступлений против информационной безопасности.	выявлять факты и обстоятельства, требующие правовой квалификации, правильно определять круг нормативно-правовых актов, нормы которых распространяются на данные факты и обстоятельства, давать юридическую оценку преступлениям против основ национальной безопасности, в том числе при квалификации преступлений против информационной безопасности.	навыками грамотного юридического анализа фактов, событий и обстоятельств и юридически правильной квалификации преступлений против основ национальной безопасности, в том числе. преступления против информационной безопасности.

## 2. Структура и содержание дисциплины

### 2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зач.ед. (144 часа), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид учебной работы	Всего часов	Семестры (часы)			
		7	-	-	-
<b>Контактная работа, в том числе:</b>	<b>50.3</b>	<b>50.3</b>	-	-	-
<b>Аудиторные занятия (всего):</b>	44	44	-	-	-
Занятия лекционного типа	18	18	-	-	-
Лабораторные занятия	-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)	26	26	-	-	-
<b>Иная контактная работа:</b>	<b>6,3</b>	<b>6,3</b>	-	-	-
Контроль самостоятельной работы (КСР)	6	6	-	-	-
Промежуточная аттестация (ИКР)	0,3	0,3	-	-	-
<b>Самостоятельная работа, в том числе:</b>	58	58			
<i>Курсовая работа</i>	не предусмотрена	не предусмотрена	-	-	-
<i>Проработка учебного (теоретического) материала</i>	16	16	-	-	-
<i>Контрольное решение задач</i>	14	14	-	-	-
<i>Выполнение индивидуальных заданий (подготовка сообщений, презентаций)</i>	8	8	-	-	-
<i>Подготовка реферата</i>	8	8			
Подготовка к текущему контролю	12	12	-	-	-
<b>Контроль:</b>	<b>35.7</b>	<b>35.7</b>			
Подготовка к экзамену	35.7	35.7	-	-	-
<b>Общая трудоемкость</b>	<b>Час.</b>	<b>144</b>	<b>144</b>	-	-
	<b>В том числе контактная работа</b>	<b>50.3</b>	<b>50.3</b>	-	-
	<b>Зач. ед.</b>	<b>4</b>	<b>4</b>	-	-

### 2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 8 семестре (для студентов ОФО)

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Информационная безопасность как объект уголовно-правовой охраны	16	2	4		10

2.	Понятие и система преступлений против информационной безопасности по российскому уголовному законодательству	16	2	4		10
3.	Уголовно-правовая характеристика преступлений против информационной безопасности по УК РФ	16	4	4		10
4.	Квалификация преступлений против информационной безопасности	20	4	6		10
5.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты информационной безопасности	18	4	4		10
6.	Криминологические основы противодействия преступлениям против информационной безопасности	14	2	4		8
<i>Итого по дисциплине:</i>			18	26		58

### 2.3 Содержание разделов дисциплины:

#### 2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Формат текущего контроля
1.	Информационная безопасность как объект уголовно-правовой охраны	<p>1. Информационные отношения как предмет правового регулирования.</p> <p>2. Понятие информационной безопасности. Источники угроз информационной безопасности.</p> <p>3. Структура информационной безопасности как объекта уголовно - правовой охраны.</p> <p>4. Информация как объект информационных отношений предмет преступлений против информационной безопасности. Категории информации по критериям доступа к ней и распространения.</p> <p>5. Законодательство РФ в области обеспечения информационной безопасности</p>	К, Р, С



2.	<p>Понятие и система преступлений против информационной безопасности по российскому уголовному законодательству.</p>	<p>1. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. Понятие киберпреступности.</p> <p>2. Система преступлений против информационной безопасности по российскому уголовному законодательству.</p> <p>3. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.</p>	Р, П, С
3.	<p>Уголовно-правовая характеристика преступлений против информационной безопасности по УК РФ</p>	<p>Неправомерный доступ к компьютерной информации (ст. 272 УК).</p> <p>2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).</p> <p>3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).</p> <p>4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).</p> <p>5. Иные преступления, совершаемые с применением компьютерных технологий</p>	Р, КРЗ
4.	<p>Квалификация преступлений против информационной безопасности</p>	<p>1. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.</p> <p>2. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.</p> <p>3. Квалифицированные виды преступлений в сфере компьютерной информации и их</p>	Р, КРЗ

		<p>уголовно – правовая оценка.          Типовые квалифицирующие признаки.</p> <p>4. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).</p> <p>5. Проблемы квалификации иных преступлений против информационной безопасности.</p>	
5.	<p>Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты информационной безопасности</p>	<p>1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах.</p> <p>2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.</p> <p>3. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.</p> <p>4. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.).</p> <p>5. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).</p>	Р, С
6.	<p>Криминологические основы противодействия преступлениям против информационной безопасности</p>	<p>1. Современная криминологическая оценка преступности в сфере информационной безопасности.</p> <p>2. Причины и условия преступлений против информационной безопасности.</p> <p>3. Криминологические особенности личности</p>	Р, С

		преступника в сфере информационной безопасности и механизм преступного поведения. 4. Основные направления и меры предупреждения преступлений против информационной безопасности.	
--	--	---	--

### 2.3.2 Занятия семинарского типа

№ раздела	Наименование раздела	Тематика практических занятий (семинаров)	Формат текущего контроля
1.	Информационная безопасность как объект уголовно-правовой охраны	<p><b>Занятие 1.</b> 1. Информационные отношения как предмет правового регулирования. 2. Понятие информационной безопасности. Источники угроз информационной безопасности. 3. Структура информационной безопасности как объекта уголовно - правовой охраны.</p> <p><b>Занятие 2.</b> 4. Информация как объект информационных отношений предмет преступлений против информационной безопасности. Категории информации по критериям доступа к ней и распространения. 5. Законодательство РФ в области обеспечения информационной безопасности 6. Основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации в области уголовно-правовой охраны информационной безопасности.</p>	Ответ на семинаре, коллоквиум, сообщение, реферат
2.	Понятие и система преступлений против информационной безопасности по российскому уголовному законодательству.	<p><b>Занятие 1.</b> 1. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. 2. Понятие киберпреступности.</p> <p><b>Занятие 2.</b></p>	Ответ на семинаре, сообщение, реферат, презентация

		<p>3. Система преступлений против информационной безопасности по российскому уголовному законодательству.</p> <p>4. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.</p> <p>5. Выявление и юридическая оценка фактов, событий и обстоятельств при квалификации преступлений против информационной безопасности.</p>	
3.	Уголовно-правовая характеристика преступлений против информационной безопасности по УК РФ	<p><b>Занятие 1.</b></p> <p>1. Неправомерный доступ к компьютерной информации (ст. 272 УК).</p> <p>2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).</p> <p>3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).</p> <p><b>Занятие 2.</b></p> <p>4. Иные преступления против информационной безопасности по УК РФ.</p> <p>5. Преступления против информационной безопасности, совершаемые с использованием глобальных компьютерных сетей.</p> <p>6. Выявление и юридическая оценка фактов, событий и обстоятельств при квалификации преступлений против информационной безопасности.</p> <p>7. Квалификация фактов, событий и обстоятельства, связанных с совершением преступлений против основ информационной безопасности.</p>	Ответ на семинаре, реферат, контрольное решение задач
4.	Квалификация преступлений против информационной безопасности	<p><b>Занятие 1.</b></p> <p>1. Проблемы квалификации преступлений в сфере компьютерной информации по</p>	Ответ на семинаре, реферат, контрольное решение задач

		<p>объекту (предмету) и объективной стороне.</p> <p>2. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.</p> <p><b>Занятие 2.</b></p> <p>3. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка. Типовые квалифицирующие признаки.</p> <p><b>Занятие 3.</b></p> <p>4. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).</p> <p>5. Проблемы квалификации иных преступлений против информационной безопасности.</p> <p>6. Выявление и юридическая оценка фактов, событий и обстоятельств при квалификации преступлений против информационной безопасности.</p> <p>7.Квалификация фактов, событий и обстоятельства, связанных с совершением преступлений против основ информационной безопасности.</p>	
5.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты информационной безопасности	<p><b>Занятие 1.</b></p> <p>1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах.</p> <p>2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.</p> <p>3. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.</p>	Ответ на семинаре, сообщение, реферат

		<p><b>Занятие 2.</b></p> <p>4. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.).</p> <p>5. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).</p> <p>6. Выявление и юридическая оценка фактов, событий и обстоятельств при квалификации преступлений против информационной безопасности в зарубежном и международном уголовном законодательстве.</p> <p>7. Квалификация фактов, событий и обстоятельства, связанных с совершением преступлений против основ информационной безопасности в зарубежном и международном уголовном законодательстве.</p>	
6.	Криминологические основы противодействия преступлениям против информационной безопасности	<p><b>Занятие 1.</b></p> <p>1. Современная криминологическая оценка преступности в сфере информационной безопасности.</p> <p>2. Причины и условия преступлений против информационной безопасности.</p> <p><b>Занятие 2.</b></p> <p>3. Криминологические особенности личности преступника в сфере информационной безопасности и механизм преступного поведения.</p> <p>4. Основные направления и меры предупреждения преступлений против информационной безопасности.</p> <p>5. Выявление и юридическая оценка фактов, событий и</p>	Ответ на семинаре, сообщение, реферат

		<p>обстоятельств в изучении криминологических основ противодействия преступлениям против информационной безопасности</p> <p>6. Требования нормативных правовых актов в области защиты государственной тайны в изучении криминологических основ противодействия преступлениям против информационной безопасности.</p>	
--	--	--	--

### 2.3.3 Лабораторные занятия

Лабораторные занятия не предусмотрены.

### 2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

## 2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	Методические указания для обучающихся по освоению дисциплин кафедры уголовного права и криминологии, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой уголовного права и криминологии, протокол № 18 от 13 апреля 2018 г.
2	Контрольное решение задач	Методические указания для обучающихся по освоению дисциплин кафедры уголовного права и криминологии, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой уголовного права и криминологии, протокол № 18 от 13 апреля 2018 г.
3	Подготовка сообщений, презентаций	Методические указания для обучающихся по освоению дисциплин кафедры уголовного права и криминологии, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой уголовного права и криминологии, протокол № 18 от 13 апреля 2018 г.
4	Выполнение реферата	Методические указания для обучающихся по освоению дисциплин кафедры уголовного права и криминологии, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой уголовного права и криминологии, протокол № 18 от 13 апреля 2018 г.
5	Подготовка к текущему контролю	Методические указания для обучающихся по освоению дисциплин кафедры уголовного права и криминологии, в том числе по организации самостоятельной работы студентов, утвержденные кафедрой уголовного права и криминологии, протокол № 18 от 13 апреля 2018 г.
6	Подготовка к коллоквиуму	Методические указания для обучающихся по освоению дисциплин кафедры уголовного права и криминологии, в том

		числе по организации самостоятельной работы студентов, утвержденные кафедрой уголовного права и криминологии, протокол № 18 от 13 апреля 2018 г.
--	--	--

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

### **3. Образовательные технологии**

При изучении дисциплины «Компьютерные преступления» применяются такие образовательные технологии, используемые при реализации различных видов учебной работы, как проблемная лекция, лекция-визуализация, сообщение, коллоквиум контрольное решение задач (разбор конкретных ситуаций).

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

## **4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации**

### **4.1 Фонд оценочных средств для проведения текущей аттестации**

*Примерные контрольные вопросы по теме «Информационная безопасность как объект уголовно-правовой охраны».*

Дайте характеристику информационным отношениям как предмету правового регулирования.

2. Дайте понятие информационной безопасности. Назовите источники угроз информационной безопасности.

3. Определите структуру информационной безопасности как объекта уголовно - правовой охраны.

4. Дайте понятие информации как предмета преступлений против информационной безопасности. Назовите категории информации по критериям доступа к ней и распространения.

5. Дайте характеристику законодательства РФ в области обеспечения информационной безопасности

*Примерные контрольные вопросы по теме «Понятие и система преступлений против информационной безопасности по российскому уголовному законодательству».*

1. Дайте характеристику эволюции уголовного законодательства, предусматривающего ответственность преступлений против информационной безопасности в России.



2. Дайте понятие преступлений против информационной безопасности и определите их место в системе информационных преступлений.
3. Дайте понятие киберпреступности.
4. Определите систему преступлений против информационной безопасности по российскому уголовному законодательству.
5. Определите соотношение и взаимосвязь преступлений против информационной безопасности и преступлений в сфере компьютерной информации.

### *Примерные темы сообщений и рефератов*

1. Криминологическая характеристика преступлений в сфере компьютерной информации.
2. Анализ воздействия киберпреступности на финансовый и иные сектора экономики.
3. Взаимодействие компьютерной и организованной преступности.
4. Виды и классификация преступлений совершаемых с использованием компьютерных технологий.
5. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
6. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).
7. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).
8. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).
9. Иные преступления, совершаемые с применением компьютерных технологий.
10. Перспективные направления совершенствования уголовного законодательства об ответственности за преступления в сфере компьютерной информации.
11. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.
12. Преступления в сфере компьютерной информации по законодательству стран континентальной системы права.
13. Преступления в сфере компьютерной информации по законодательству стран англо-саксонской системы права.
14. Преступления в сфере компьютерной информации по законодательству стран мусульманской системы права.
15. Причины и условия преступлений в сфере компьютерной информации в историческом аспекте.
16. Криминологическая характеристика личности преступника в сфере компьютерной информации.
17. Особенности личности преступника, совершающего преступления в глобальных компьютерных сетях.
18. Борьба с компьютерной преступностью: организационные, правовые и методические аспекты.
19. Перспективы совершенствование системы борьбы с киберпреступностью.
20. Место и роль технических и программных средств в профилактике компьютерных преступлений.
21. Международное сотрудничество в борьбе с киберпреступностью.
22. Особенности правового регулирования борьбы с преступлениями в сфере компьютерной информации в Японии.
23. Особенности правового регулирования борьбы с преступлениями в сфере компьютерной информации в США.
24. Особенности правового регулирования борьбы с преступлениями в сфере компьютерной информации в Германии.

25. Особенности правового регулирования борьбы с преступлениями в сфере компьютерной информации в странах СНГ..

***Примерные вопросы для коллоквиума по теме «Информационная безопасность как объект уголовно-правовой охраны»***

1. Информационные отношения как предмет правового регулирования.
2. Понятие информационной безопасности. Источники угроз информационной безопасности.
3. Структура информационной безопасности как объекта уголовно - правовой охраны.
4. Информация как объект информационных отношений предмет преступлений против информационной безопасности. Категории информации по критериям доступа к ней и распространения.
5. Законодательство РФ в области обеспечения информационной безопасности
6. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. Понятие киберпреступности.

***Примерные задачи для решения на семинарских занятиях***

**№ 1**

М. и Л., имеющие специальные познания в области электроники и компьютерной техники, по предварительному сговору между собой осуществили несанкционированное подключение при помощи технических средств к базе данных компьютерной информации пользователей, находящейся на машинном носителе в сети электронно-вычислительных машин (ЭВМ) компании сотовой телефонной связи.

При помощи неправомерно полученной таким образом компьютерной информации М. и Л. осуществляли без оплаты телефонные переговоры за счет денежных средств клиентов (пользователей) названной компании, имеющих законный доступ к компьютерной информации сети сотовой телефонной связи, а также предоставляли такую возможность третьим лицам.

Квалифицируйте содеянное

**№ 2**

Ф., имеющий специальные познания в области электроники и компьютерной техники, желая извлечь незаконную выгоду, с целью несанкционированного проникновения при помощи технических средств к базе данных компьютерной информации пользователей, находящейся на машинном носителе в сети электронно-вычислительных машин компании мобильной связи, кустарным способом изготовил интерфейсы, предназначенные для связи компьютера через последовательный порт с телефоном ЛС-300. С помощью этих технических средств и специальной компьютерной программы осуществил копирование информации, содержащейся на микропроцессоре телефонного аппарата, на свой телефонный аппарат, чем нарушил охраняемые законом права и интересы компании мобильной связи и произвел модификацию информации.

Квалифицируйте содеянное

**№ 3**

Ш. совместно с К. незаконно получили абонентские номера и шифр-коды сотовых телефонов клиентов фирмы ОАО. Ш., К. и неустановленные следствием лица произвели кодировку имевшихся у них сотовых телефонов шифр-кодами клиентов фирмы ОАО.

Ш. совместно с К., периодически изменяя при помощи специальной схемы перекодировки шифр-код и номер телефона, многократно использовал имеющийся у них

сотовый телефон как лично, так и предоставляя гражданам для осуществления переговоров, взимая плату из расчета 4 р. за минуту разговора по международной, междугородней и внутригородской связи, чем причинили имущественный ущерб владельцу радиоканалов – фирме ОАО на сумму 449 992, 45 р., в виде взысканной с фирмы ОАО предприятием «К» платы за использование технических каналов связи, а также уплаченных налогов и неполученной оплаты за абонентское использование указанного радиотелефона.

При предоставлении в этот период услуг всех видов сотовой связи неограниченному кругу лиц происходило блокирование каналов связи клиентам указанной фирмы, нарушение работы ЭВМ, что делало невозможным доступ пользователей к услугам сотовой связи ОАО на период незаконно ведущихся переговоров.

Не имея специального разрешения на предоставление услуг всех видов сотовой связи неограниченному кругу лиц, Ш. и К. незаконно получили информацию, к которой нет свободного доступа, составляющую сведения об абонентских номерах и шифр-кодах сотовых телефонов клиентов фирмы ОАО, относящуюся к коммерческой тайне и доступную лишь ограниченному кругу сотрудников названного общества.

Квалифицируйте содеянное

#### **4.2 Фонд оценочных средств для проведения промежуточной аттестации**

##### **ПРИМЕРНЫЙ ПЕРЕЧЕНЬ**

##### **вопросов для изучения дисциплины «Преступления против информационной безопасности»**

- 1 Информационные отношения как предмет правового регулирования.
- 2 Понятие информационной безопасности. Источники угроз информационной безопасности.
- 3 Структура информационной безопасности как объекта уголовно - правовой охраны.
- 4 Информация как объект информационных отношений предмет преступлений против информационной безопасности. Категории информации по критериям доступа к ней и распространения.
- 5 Основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации в области уголовно-правовой охраны информационной безопасности.
- 6 Понятие преступлений против информационной безопасности, их место в системе информационных преступлений.
- 7 Система преступлений против информационной безопасности по российскому уголовному законодательству.
- 8 Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.
- 9 Особенности объекта и предмета преступлений против информационной безопасности
- 10 Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
- 11 Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).
- 12 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).
- 13 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).
- 14 Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.

15 Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.

16 Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка. Типовые квалифицирующие признаки.

17 Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).

18 Проблемы квалификации иных преступлений против информационной безопасности.

19 Отграничение преступлений против информационной безопасности от смежных составов преступлений.

20 5. Выявление и юридическая оценка фактов, событий и обстоятельств при квалификации эпеступлений против информационной безопасности.

21 Квалификация фактов, событий и обстоятельства, связанных с совершением преступлений против основ информационной безопасности.

22 Общая характеристика международного законодательства в сфере борьбы с киберпреступностью.

23 Понятие киберпреступности в международном уголовном праве.

24 Основные направления международного сотрудничества в борьбе с киберпреступностью.

25 Ответственность за преступления против информационной безопасности в странах СНГ.

26 22. Выявление и юридическая оценка фактов, событий и обстоятельств при квалификации преступлений против информационной безопасности в зарубежном и международном уголовном законодательстве.

27 22. Квалификация фактов, событий и обстоятельства, связанных с совершением преступлений против основ информационной безопасности в зарубежном и международном уголовном законодательстве.

28 Органы, осуществляющие борьбу с преступлениями против информационной безопасности .

29 Особенности борьбы преступлениями против информационной безопасности в глобальных компьютерных сетях.

30 Состояние, уровень, структура, динамика преступлений против информационной безопасности.

31 Причины и условия преступлений против информационной безопасности в современных условиях.

32 Характеристика личности преступника в сфере информационной безопасности.

33 Законодательство РФ в области обеспечения информационной безопасности

34 Основы предупреждения преступлений против информационной безопасности .

35 Правовое регулирование борьбы с преступлениями против информационной безопасности .

36 Принципы борьбы с преступлениями против информационной безопасности.

37 Основные направления предупреждения преступлений против информационной безопасности.

38 Выявление и юридическая оценка фактов, событий и обстоятельств в изучении криминологических основ противодействия преступлениям против информационной безопасности

39 Требования нормативных правовых актов в области защиты государственной тайны в изучении криминологических основ противодействия преступлениям против информационной безопасности.

### Критерии оценки экзамена

Оценка «отлично» выставляется студенту, если студентом дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по теме, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.

Оценка «хорошо» выставляется студенту, если студентом дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной гистологической терминологии. Могут быть допущены 2–3 неточности или незначительные ошибки, исправленные обучающимся с помощью преподавателя.

Оценка «удовлетворительно» выставляется при недостаточно полном и недостаточно развернутом ответе. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано.

Оценка «неудовлетворительно» выставляется при несоответствии ответа заданному вопросу, использовании при ответе ненадлежащих нормативных и иных источников, когда ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

## 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

### 5.1.1. Нормативные правовые акты<sup>1</sup>:

1. Конституция Российской Федерации 1993 г. (с погр.) // URL: <http://www.constitution.ru/>
2. Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г. // СЗ РФ. 2004. № 40. Ст. 3882. // Сайт ООН: [http://www.un.org/ru/documents/decl\\_conv/conventions/orgcrime](http://www.un.org/ru/documents/decl_conv/conventions/orgcrime)
3. Международная конвенция о борьбе с финансированием терроризма 1999 г. // Веб-сайт ООН. – URL: [http://www.un.org/ru/documents/decl\\_conv/conventions/terfin.shtml](http://www.un.org/ru/documents/decl_conv/conventions/terfin.shtml)
4. Конвенция Совета Европы об отмывании, выявлении, конфискации доходов от преступной деятельности и финансировании терроризма 2005 г. // <http://base.garant.ru/2570351/cc384117f448d63c9e26583848a7abd0/>.
5. Международная Конвенция о киберпреступности (Будапешт, 23 ноября 2001 г.) // [https://online.zakon.kz/Document/?doc\\_id=30170556](https://online.zakon.kz/Document/?doc_id=30170556)
6. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (Страсбург, 28 января 2003 г.) // [https://online.zakon.kz/Document/?doc\\_id=30170556](https://online.zakon.kz/Document/?doc_id=30170556)
7. Уголовный кодекс Российской Федерации 1996 г. (в действующей редакции) // Официальный интернет-портал правовой информации [Официальный портал] – URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102041891>.
8. О безопасности: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ // Президент РФ [Официальный сайт] – URL: <http://kremlin.ru/acts/bank/32417>.
9. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ // Президент РФ [Официальный сайт] – URL: <http://kremlin.ru/acts/bank/19708>
10. О государственной тайне: Закон РФ от 21.07.93 г. № 5485-1 // [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_2481/](http://www.consultant.ru/document/cons_doc_LAW_2481/)
11. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. 149-ФЗ // Президент РФ [Официальный сайт] – URL: <http://kremlin.ru/acts/bank/24157>
12. О персональных данных: Федеральный закон от 27.07.2006 г. № 152-ФЗ // Президент РФ [Официальный сайт] – URL: <http://kremlin.ru/acts/bank/24157>
13. О перечне сведений, отнесенных к государственной тайне: Указ Президента РФ от 11.02.2006 г. № 90 (ред. от 22.11.2016 г. № 614) // Президент РФ [Официальный сайт] – URL: <http://kremlin.ru/acts/bank/23430/page/1>

### 5.1.2 Основная литература

1. Российское уголовное право. Общая часть: Учебник для вузов / под ред. В.П. Коняхина и М.Л. Прохоровой. М.: Контракт, 2014 // Электронно-библиотечная система «Знаниум»: <http://znanium.com/catalog.php?bookinfo=674051>.
2. Российское уголовное право. Особенная часть: Учебник для вузов / под ред. В.П. Коняхина и М.Л. Прохоровой. М., Контракт, 2015 // Электронно-библиотечная система «Знаниум»: <http://znanium.com/catalog.php?bookinfo=674053>.
3. Козаченко И.Я., Новоселов Г.П. Уголовное право. Особенная часть в 2 т. Том 2:

---

<sup>1</sup> Преподавателем может быть предложен дополнительный перечень нормативно-правовых актов применительно к отдельным темам дисциплины.

учебник для бакалавриата и специалитета. 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2017. (Серия: бакалавр и специалист) // <https://biblio-online.ru/book/EB38D499-CD45-439C-AE73-E7DDCAFE9511>.

4. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В.Г. Степанов-Егиянц. —М.: СТАТУТ, 2016. / Режим доступа: <https://e.lanbook.com/book/92503>.

5. Уголовное право зарубежных стран в 3 т. Том 3. Особенная часть : учебник для бакалавриата и магистратуры / Н. Е. Крылова [и др.] ; отв. ред. Н. Е. Крылова. — 5-е изд., пер. и доп. — М. : Издательство Юрайт, 2018. (Серия : Бакалавр и магистр. Академический курс). / Режим доступа : [www.biblio-online.ru/book/BF9DE008-FF1A-4DDC-8DD4-5AACC8C758AD](http://www.biblio-online.ru/book/BF9DE008-FF1A-4DDC-8DD4-5AACC8C758AD).

### 5.1.3 Дополнительная литература

1. Баглай Ю.В. Квалификация отдельных видов преступлений [Электронный ресурс] : учебное пособие / Ю.В. Баглай. —Оренбург : ОГУ, 2015. / Режим доступа: <https://e.lanbook.com/book/98030>.

2. Дуюнов В.К. Хлебушкин А. Г. Квалификация преступлений: законодательство, теория, судебная практика: Монография / Дуюнов В.К., Хлебушкин А.Г., - 4-е изд. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019./ Режим доступа: <http://znanium.com/catalog/product/923814>

3. Колосовский В.В. Теоретические проблемы квалификации уголовно-правовых деяний [Электронный ресурс] : монография / В.В. Колосовский. —Москва : СТАТУТ, 2011. / Режим доступа: <http://znanium.com/catalog/product/330691>

4. Комментарий к Уголовному кодексу РФ в 4 т. Том 2. Особенная часть. Разделы VII—VIII / В. М. Лебедев [и др.] ; отв. ред. В. М. Лебедев. — М. : Издательство Юрайт, 2017. — 371 с. — (Серия : Профессиональные комментарии). — ISBN 978-5-534-00046-7.<https://biblio-online.ru/book/06EFC8F3-1E88-470B-B1B7-3A4EB7173CB6>

5. Международное уголовное право : учебник для бакалавриата и магистратуры / А. В. Наумов, А. Г. Кибальник, В. Н. Орлов, П. В. Волосюк ; под ред. А. В. Наумова, А. Г. Кибальника. 3-е изд., перераб. и доп. М. : Издательство Юрайт, 2017. (Серия : Бакалавр и магистр. Академический курс). <https://biblio-online.ru/book/BC04B8D7-76B4-45C0-937A-90BBV9983D7C>.

6. Преступления против общественной безопасности и общественного порядка : учебное пособие для бакалавриата и магистратуры / А. В. Наумов [и др.] ; отв. ред. А. В. Наумов, А. Г. Кибальник. — М. : Издательство Юрайт, 2017. — 141 с. — (Серия : Бакалавр и магистр. Модуль.) // <https://biblio-online.ru/book/ADEC603A-04D4-4BB5-950E-348AA337F3F6>

7. Сверчков, В. В. Курс уголовного права. Общая часть в 2 книгах [Электронный ресурс]: учебник для бакалавриата и магистратуры / В. В. Сверчков ; под ред. В. Т. Томина. — М. : Издательство Юрайт, 2016. — 815 с. — Режим доступа : [www.biblio-online.ru/book/23CD4F39-4F76-478C-A9B9-CE7D41E0BF95](http://www.biblio-online.ru/book/23CD4F39-4F76-478C-A9B9-CE7D41E0BF95)

8. Чекунов И.Г. Киберпреступность: понятие и классификация// Российский следователь. 2012. N 2. [Электронный ресурс]. Режим доступа: <http://www.center-bereg.ru/h583.html>

9. О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации: постановление Пленума Верховного Суда РФ от 10 октября 2003 г. № 5 // Верховный Суд Российской Федерации [Официальный сайт] — URL: <http://www.supcourt.ru/documents/own/8334/>.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань», «Знаниум» и «Юрайт».

#### 5.4. Периодические издания:

1. Вестник Краснодарского университета МВД России. – URL: [https://xn--d1alsn.xn--b1aew.xn--p1ai/Nauka/Redakcionno\\_izdatelskaja\\_dejatelnost/Nauchno\\_prakticheskij\\_zhurnal\\_Vestnik\\_Kr/Arhiv\\_zhurnalov](https://xn--d1alsn.xn--b1aew.xn--p1ai/Nauka/Redakcionno_izdatelskaja_dejatelnost/Nauchno_prakticheskij_zhurnal_Vestnik_Kr/Arhiv_zhurnalov).
2. Вестник Омского государственного университета. Серия «Право». – URL: [http://www.omlaw.ru/index.php?option=com\\_content&view=category&id=90&Itemid=331](http://www.omlaw.ru/index.php?option=com_content&view=category&id=90&Itemid=331).
3. Гуманитарные, социально-экономические и общественные науки // Архив журналов. Выпуски текущего года. Новый номер. – URL: <http://www.online-science.ru>
4. Научные ведомости БелГУ. – URL: <http://nv.bsu.edu.ru/nv/mag/03/archive/>.
5. Общество и право. – URL: [https://xn--d1alsn.xn--b1aew.xn--p1ai/Nauka/Redakcionno\\_izdatelskaja\\_dejatelnost/Obshhestvo\\_i\\_pravo/Arhiv\\_zhurnalov](https://xn--d1alsn.xn--b1aew.xn--p1ai/Nauka/Redakcionno_izdatelskaja_dejatelnost/Obshhestvo_i_pravo/Arhiv_zhurnalov).
6. Общество: политика, экономика, право. – URL: <http://www.dom-hors.ru/arhiv-zhurnala-politika-ekonomika-pravo/>.
7. Северо-Кавказский юридический вестник. – URL: <http://vestnik.uriu.ranepa.ru/archives/>.
8. Теория и практика общественного развития. – URL: <http://teoria-practica.ru/arhiv-zhurnala/>.
9. Бизнес. Образование. Право. Вестник Волгоградского института бизнеса // <http://vestnik.volbi.ru/webarchive/numbers>.

#### 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Кубанский государственный университет [Официальный сайт] – URL: <http://www.law.kubsu.ru>.
2. ООН [Официальный портал] – URL: <http://www.un.org/ru>.
3. Совет Европы <http://www.coe.int/ru>.
4. СНГ [Официальный портал] – URL: <http://www.e-cis.info>.
5. Официальный интернет-портал правовой информации [Официальный портал] – URL: <http://www.pravo.gov.ru>.
6. Президент РФ [Официальный сайт] – URL: <http://www.kremlin.ru>.
7. Государственная Дума Федерального Собрания Российской Федерации [Официальный сайт] – URL: <http://www.duma.gov.ru>.
8. Совет Федерации Федерального Собрания Российской Федерации [Официальный сайт] – URL: <http://www.council.gov.ru>.
9. Правительство РФ [Официальный сайт] [Официальный портал] – URL: – URL: <http://www.правительство.рф> или <http://www.government.ru>.
10. Конституционный Суд Российской Федерации [Официальный сайт] – URL: <http://www.ksrf.ru>.
11. Верховный Суд Российской Федерации [Официальный сайт] – URL: <http://www.supcourt.ru>.
12. «Юридическая Россия» – федеральный правовой портал [Официальный портал] – URL: <http://law.edu.ru>.
13. Российская государственная библиотека [Официальный сайт] – URL: <http://www.rsl.ru>.



## 7. Методические указания для обучающихся по освоению дисциплины (модуля)

При изучении дисциплины «Преступления против информационной безопасности» необходимо руководствоваться действующим федеральным и иным законодательством и разработанными на его основе подзаконными нормативными актами.

Изучение курса осуществляется в тесном взаимодействии с другими юридическими и общественными дисциплинами. Форма и способы изучения материала определяются с учетом специфики изучаемой темы. Однако во всех случаях необходимо обеспечить сочетание изучения теоретического материала, научного толкования того или иного понятия, даваемого в учебниках и лекциях, с самостоятельной работой студентов, выполнением практических заданий, подготовкой сообщений и докладов.

Важную роль играет ознакомление с судебной-следственной практикой расследования и рассмотрения уголовных дел.

### *Методические указания по лекционным занятиям*

В ходе лекции студентам рекомендуется конспектировать ее основные положения, не стоит пытаться дословно записать всю лекцию, поскольку скорость лекции не рассчитана на аутентичное воспроизведение выступления лектора в конспекте. Тем не менее, она является достаточной для того, чтобы студент смог не только усвоить, но и зафиксировать на бумаге сущность затронутых лектором проблем, выводы, а также узловые моменты, на которые обращается особое внимание в ходе лекции. Основным средством работы на лекционном занятии является конспектирование. Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста. Результат конспектирования – запись, позволяющая студенту немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других. Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей концепции лекции (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т.е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Определения, которые дает лектор, стоит по возможности записать дословно и выделить другим цветом или же подчеркнуть. В случае изложения лектором хода научной дискуссии желательно кратко законспектировать существо вопроса, основные позиции и фамилии ученых, их отстаивающих. Если в обоснование своих выводов лектор приводит ссылки на справочники, статистические данные, нормативные акты и другие официально опубликованные сведения, имеет смысл лишь кратко отразить их существо и указать источник, в котором можно полностью почерпнуть излагаемую информацию.

Во время лекции студенту рекомендуется иметь на столах помимо конспектов также программу спецкурса, которая будет способствовать развитию мнемонической памяти, возникновению ассоциаций между выступлением лектора и программными

вопросами, Уголовный кодекс РФ, иные необходимые законы и подзаконные акты, поскольку гораздо эффективнее следить за ссылками лектора на нормативный акт по его тексту, нежели пытаться воспринять всю эту информацию на слух.

В случае возникновения у студента по ходу лекции вопросов, их следует записать и задать в конце лекции в специально отведенное для этого время.

По окончании лекции (в тот же или на следующий день, пока еще в памяти сохранилась информация) студентам рекомендуется доработать свои конспекты, привести их в порядок, дополнить сведениями с учетом дополнительно изученного нормативного, справочного и научного материала. Крайне желательно на полях конспекта отмечать не только изученные точки зрения ученых по рассматриваемой проблеме, но и выражать согласие или несогласие самого студента с законспектированными положениями, материалами судебной практики и т.п.

Лекционное занятие предназначено для изложения особенно важных, проблемных, актуальных в современной науке вопросов. Лекция, также как и семинарское, практическое занятие, требует от студентов определенной подготовки. Студент обязательно должен знать тему предстоящего лекционного занятия и обеспечить себе необходимый уровень активного участия: подобрать и ознакомиться, а при необходимости иметь с собой рекомендуемый преподавателем нормативный материал, повторить ранее пройденные темы по вопросам, которые будут затрагиваться в предстоящей лекции, вспомнить материал иных дисциплин. В частности, большое значение имеет подготовка по курсу «Теория государства и права», «Конституционное право».

Применение отдельных образовательных технологий требует специальной подготовки не только от преподавателя, но и участвующих в занятиях студентов. Так, при проведении лекции-дискуссии, которая предполагает разделение присутствующих студентов на группы, студент должен быть способен высказать свою позицию относительно выдвинутых преподавателем точек зрения.

*Методические указания для подготовки  
к практическим занятиям*

Для практических (семинарских занятий) по дисциплине «Преступления против личности» характерно сочетание теории с решением задач (казусов), анализом приговоров по конкретным уголовным делам.

Семинарские (практические) занятия представляют собой одну из важных форм самостоятельной работы студентов над нормативными актами, материалами местной и опубликованной судебной практики, научной и учебной литературой непосредственно в учебной аудитории под руководством преподавателя.

В зависимости от изучаемой темы и ее специфики преподаватель выбирает или сочетает следующие формы проведения семинарских (практических) занятий: обсуждение теоретических вопросов, подготовка рефератов, решение задач (дома или в аудитории), круглые столы, научные дискуссии с участием практических работников и ученых и т.п. Проверка усвоения отдельных (ключевых) тем может осуществляться посредством проведения коллоквиума.

Подготовка к практическому занятию заключается в подробном изучении конспекта лекции, нормативных актов и материалов судебной практики, рекомендованных к ним, учебной и научной литературы, основные положения которых студенту рекомендуется конспектировать.

Активное участие в работе на практических и семинарских занятиях предполагает выступления на них, дополнение ответов однокурсников, коллективное обсуждение спорных вопросов и проблем, что способствует формированию у студентов навыков формулирования, аргументации и отстаивания выработанного решения, умения его защитить в дискуссии и представить дополнительные аргументы в его пользу. Активная

работа на семинарском (практическом) занятии способствует также формированию у студентов навыков публичного выступления, умения ясно, последовательно, логично и аргументировано излагать свои мысли.

При выступлении на семинарских или практических занятиях студентам разрешается пользоваться конспектами для цитирования нормативных актов, судебной практики или позиций ученых. По окончании ответа другие студенты могут дополнить выступление товарища, отметить его спорные или недостаточно аргументированные стороны, проанализировать позиции ученых, о которых не сказал предыдущий выступающий.

В конце занятия после подведения его итогов преподавателем студентам рекомендуется внести изменения в свои конспекты, отметить информацию, прозвучавшую в выступлениях других студентов, дополнения, сделанные преподавателем и не отраженные в конспекте.

Практические занятия требуют предварительной теоретической подготовки по соответствующей теме: изучения учебной и дополнительной литературы, ознакомления с нормативным материалом, актами толкования. Рекомендуется при этом вначале изучить вопросы темы по учебной литературе. Если по теме прочитана лекция, то непременно надо использовать материал лекции, так как учебники часто устаревают уже в момент выхода в свет.

Применение отдельных образовательных технологий требуют предварительного ознакомления студентов с содержанием применяемых на занятиях приемов. Так, при практических занятиях студент должен представлять как его общую структуру, так и особенности отдельных методических приемов: дискуссии, контрольные работы, использование правовых документов и др.

*Примерные этапы практического занятия  
и методические приемы их осуществления:*

- постановка целей занятия: обучающей, развивающей, воспитывающей;
- планируемые результаты обучения: что должны студенты знать и уметь;
- проверка знаний: устный опрос, фронтальный опрос, программированный опрос, блиц-опрос, письменный опрос, комментирование ответов, оценка знаний, обобщение по опросу;
- изучение нового материала по теме;
- закрепление материала предназначено для того, чтобы студенты запомнили материал и научились использовать полученные знания (активное мышление).

Формы закрепления:

- решение задач;
- работа с приговорами судов;
- групповая работа (коллективная мыслительная деятельность).

Домашнее задание:

- работа над текстом учебника;
- решение задач.

В рамках семинарского занятия студент должен быть готов к изучению предлагаемых правовых документов и их анализу.

В качестве одного из оценочных средств в рамках практических занятий может использоваться *контрольная работа*.

Для проведения *контрольной работы* в рамках практических занятий студент должен быть готов ответить на проблемные вопросы, проявить свои аналитические способности. При ответах на вопросы контрольной работы в обязательном порядке необходимо:

- правильно уяснить суть поставленного вопроса;
- сформулировать собственную позицию;

- подкрепить свой ответ ссылками на нормативные, научные, иные источники;
- по заданию преподавателя изложить свой ответ в письменной форме.

#### *Методические рекомендации по решению ситуационных задач (кейсов)*

Решения ситуационных задач относятся к поисковому методу и предполагают третий (применение) и четвертый (творчество) уровень знаний. Характеристики выбранной для ситуационной задачи проблемы и способы ее решения являются отправной точкой для оценки качества этого вида работ. В динамике обучения сложность проблемы нарастает, и к его завершению должна соответствовать сложности задач, поставленных профессиональной деятельностью на начальном этапе.

Оформляются задачи и эталоны ответов к ним письменно. Если решение задач связано с квалификацией преступления, при ответе необходимо сослаться на соответствующие положения уголовного закона, иных нормативно-правовых актов (при необходимости), использовать рекомендации, содержащиеся в постановлениях Пленума Верховного Суда РФ. Ответ должен быть полным и аргументированным.

При составлении ситуационных задач студентам рекомендуется использовать материалы опубликованной или представленной на сайте <http://sudact.ru> судебной практики.

#### *Методические рекомендации по подготовке рефератов, презентаций, сообщений*

Первичные навыки научно-исследовательской работы должны приобретаться студентами при написании рефератов по специальной тематике.

Цель: научить студентов связывать теорию с практикой, пользоваться литературой, статистическими данными, привить умение популярно излагать сложные вопросы.

Рефераты составляются в соответствии с указанными темами. Выполнение рефератов предусмотрено на листах формата А 4. Они сдаются на проверку преподавателю в соответствии с указанным графиком.

*Требования к работе.* Реферативная работа должна выявить углубленные знания студентов по той или иной теме дисциплины «Преступления против личности». В работе должно проявиться умение работать с литературой. Студент обязан изучить и использовать в своей работе не менее 2–3 книг и 1–2 периодических источника литературы.

#### *Оформление реферата:*

1. Реферат должен иметь следующую структуру: а) план; б) изложение основного содержания темы; в) список использованной литературы.
2. Общий объём – 5–7 с. основного текста.
3. Перед написанием должен быть составлен план работы, который обычно включает 2–3 вопроса. План не следует излишне детализировать, в нём перечисляются основные, центральные вопросы темы.
4. В процессе написания работы студент имеет право обратиться за консультацией к преподавателю кафедры.
5. В основной части работы большое внимание следует уделить глубокому теоретическому освещению основных вопросов темы, правильно увязать теоретические положения с практикой, конкретным фактическим и цифровым материалом.
6. В реферате обязательно отражается использованная литература, которая является завершающей частью работы.
7. Особое внимание следует уделить оформлению. На титульном листе необходимо указать название вуза, название кафедры, тему, группу, свою фамилию и инициалы, фамилию научного руководителя. На следующем листе приводится план работы.
8. При защите реферата выставляется дифференцированная оценка.
9. Реферат, не соответствующий требованиям, предъявляемым к данному виду работы, возвращается на доработку.

Качество реферата оценивается по тому, насколько полно раскрыто содержание темы, использованы первоисточники, логичное и последовательное изложение. Оценивается и правильность подбора основной и дополнительной литературы (ссылки по правилам: фамилии и инициалы авторов, название книги, место издания, издательство, год издания, страница).

Реферат должен отражать точку зрения автора на данную проблему.

Составление *презентаций* – это вид самостоятельной работы студентов по созданию наглядных информационных пособий, выполненных с помощью мультимедийной компьютерной программы PowerPoint. Этот вид работы требует навыков студента по сбору, систематизации, переработке информации, оформления ее в виде подборки материалов, кратко отражающих основные вопросы изучаемой темы, в электронном виде. Материалы презентации готовятся студентом в виде слайдов.

Одной из форм задания может быть *реферат-презентация*. Данная форма выполнения самостоятельной работы отличается от написания реферата и доклада тем, что студент результаты своего исследования представляет в виде презентации. Серией слайдов он передаёт содержание темы своего исследования, её главную проблему и социальную значимость. Слайды позволяют значительно структурировать содержание материала и одновременно заостряют внимание на логике его изложения. Слайды презентации должны содержать логические схемы реферируемого материала. Студент при выполнении работы может использовать картографический материал, диаграммы, графики, звуковое сопровождение, фотографии, рисунки и другое. Каждый слайд должен быть аннотирован, то есть он должен сопровождаться краткими пояснениями того, что он иллюстрирует. Во время презентации студент имеет возможность делать комментарии, устно дополнять материал слайдов.

Подготовка *сообщения* представляет собой разработку и представление небольшого по объему устного сообщения для озвучивания на практическом занятии. Сообщаемая информация носит характер уточнения или обобщения, несет новизну, отражает современный взгляд по определенным проблемам.

Сообщение отличается от докладов и рефератов не только объемом информации, но и ее характером – сообщения дополняют изучаемый вопрос фактическими или статистическими материалами. Возможно письменное оформление задания, оно может включать элементы наглядности (иллюстрации, демонстрацию).

Регламент времени на озвучивание сообщения – до 5 мин.

#### *Методические рекомендации по подготовке коллоквиума*

Коллоквиумом называется собеседование преподавателя и студента по заранее определенным контрольным вопросам. Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы. На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Упор делается на монографические работы профессора-автора данного спецкурса. От студента требуется:

- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- знание разных точек зрения, высказанных в научной литературе по соответствующей проблеме, умение сопоставлять их между собой;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.

Коллоквиум - это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника. Однако

коллоквиум не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной социологической литературы.

Подготовка к коллоквиуму.

Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3-4 недели. Методические указания состоят из рекомендаций по изучению источников и литературы, вопросов для самопроверки и кратких конспектов ответа с перечислением основных фактов и событий, относящихся к пунктам плана каждой темы. Это должно помочь студентам целенаправленно организовать работу по овладению материалом и его запоминанию. При подготовке к коллоквиуму следует, прежде всего, просмотреть конспекты лекций и практических занятий и отметить в них имеющиеся вопросы коллоквиума. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.

Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (2-3 человека). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, проверяет конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания. По итогам коллоквиума выставляется дифференцированная оценка по пятибалльной системе. Проведение коллоквиума позволяет студенту приобрести опыт работы над первоисточниками, что в дальнейшем поможет с меньшими затратами времени работать над литературой по курсовой работе и при подготовке к экзаменам.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

## **8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

### **8.1 Перечень информационных технологий**

Информационные технологии не предусмотрены.

### **9.1 Перечень необходимого программного обеспечения**

№№	Номер договора	Перечень лицензионного программного обеспечения
1	Дог. № 77-АЭФ/223-ФЗ/2017 от 03.11.2017	Приобретение права на использование программного продукта DesktopEducation ALNG LicSAPk MVL A Faculty EES на 2017-2018 учебный год на программное обеспечение для компьютеров и серверов Кубанского государственного университета и его филиалов:  Неисключительные права пользования сроком 1 год

		<p>(лицензия на годовую подписку) на пакет программного обеспечения «Платформа для настольных компьютеров»</p> <p>Пакет включает в себя следующие компоненты:</p> <ul style="list-style-type: none"><li>• Обновление существующей операционной системы Windows до последней версии со следующим функционалом:</li><li>• Возможность использования операционных систем в виртуальных средах на серверах сети, к которым осуществляется удаленный доступ с ПК (виртуальные рабочие столы);</li><li>• Возможность запускать одну копию в физической среде и четыре копии в виртуальных операционных средах на одном ПК</li><li>• Возможность поддержки протоколов HTTP, HTTPS, SMB, IPsec и SSL</li><li>• Возможность поддержки службы удаленного подключения внешних пользователей к внутренней локальной сети по защищенному каналу IPsec без необходимости организации каналов подключения VPN,</li><li>• Возможность выбора операционной системы с возможностью установки с носителя с интерфейсом USB, а также возможность запуска операционной системы с носителя с интерфейсом USB на любом совместимом ПК, в том числе на ПК, на котором ранее операционная система не была установлена на внутренний жесткий диск.</li><li>• Возможность использовать многоязычный пользовательский интерфейс (включая русский и английский языки) с возможностью переключения между языками в процессе работы.</li><li>• Встроенная возможность выполнения программного обеспечения, эксплуатируемого Заказчиком, без необходимости использования эмуляторов и/или средств виртуализации</li><li>• Наличие встроенной в операционную систему системы шифрования данных, с возможностью настройки необходимости ввода ключа до загрузки основных компонентов операционной системы</li><li>• Наличие встроенных групп безопасности, предусматривающих несколько уровней доступа (привилегий) к настройкам системы, с возможностью включения в них локальных пользователей</li><li>• Поддержка аппаратных средств шифрования и двухфакторной аутентификации</li><li>• Возможность централизованной настройки политик безопасности, средство для управления политиками безопасности с графическим интерфейсом</li><li>• Автоматическое распознавание съемных накопителей</li><li>• Возможность печати с учетом информации о местонахождении (автоматический выбор ближайшего принтера)</li></ul>
--	--	---

		<ul style="list-style-type: none"> <li>• Наличие встроенных механизмов изменения пользовательского интерфейса (способы ввода с клавиатуры, использование мыши, масштабирование элементов интерфейса, инструмент «экранная» лупа) для пользователей с ограниченными возможностями.</li> <li>• Настраиваемая система автоматической доставки обновлений (с выбором стратегии обновления, включая отложенную систему доставки обновлений)</li> <li>• Встроенные в ОС средства обеспечения антивирусной защиты с обновляемой базой данных о вредоносном ПО</li> <li>• Обеспечение регламентного (без использования эмуляторов и иного подобного ПО) функционирования клиентских (работающих на ПК) компонентов прикладного (специализированного) ПО, эксплуатируемого организацией, использующего, в том числе, технологии COM/COM+ и разработанного с использованием средств разработки (включая, но не ограничиваясь): VisualBasic (6.0), Delphi для среды Win32/64, неуправляемый C++, VisualFoxPro, Access</li> <li>• Обеспечение регламентного (без использования эмуляторов и иного подобного ПО) функционирования клиентских (работающих на ПК) компонентов прикладного (специализированного) ПО, эксплуатируемого организацией, использующего технологию .Net, и разработанного с использованием средств разработки (включая, но не ограничиваясь): VisualBasic .Net, C#, управляемый C++.</li> <li>• Пакет офисных приложений для работы в существующей операционной среде Windows:</li> <li>• Возможность работы с текстовыми документами (включая документы Word в том числе форматов .doc и .docx без необходимости конвертирования форматов), электронными таблицами и анализом данных с количеством строк в электронной таблице один миллион и количеством столбцов шестнадцать тысяч (включая документы Excel в том числе форматов .xls и .xlsx без необходимости конвертирования форматов), создания и проведения презентаций (включая презентации PowerPoint, в том числе форматов .ppt и .pptx без необходимости конвертирования форматов), хранения и совместной работы с текстовыми, графическими и видеозаметками. Приложения для создания и совместной работы с базами данных создания, редактирования и распространения публикаций.</li> <li>• Возможность создания электронных форм и сбора данных (совместимое с существующими порталными решениями), возможность совместной работы с документами, просмотра и редактирования их удаленно (в том числе и при отсутствии подключения к сети Интернет) с возможностью синхронизации с рабочими папками пользователя.</li> <li>• Возможность для обмена мгновенными сообщениями и уведомлении о присутствии пользователя, общего доступа к приложениям и передачи файлов, организации аудио и</li> </ul>
--	--	--



		<p>видеоконференций, а также для использования в качестве клиентского приложения системы IP-телефонии (приложение полностью совместимо с развернутой системой обмена мгновенными сообщениями, аудио и видеоконференцсвязи); набор инструментов для управления корпоративной и личной электронной почтой и установки политик хранения данных и контроля информации.</p> <ul style="list-style-type: none"> <li>• Все приложения пакета имеют возможность поддерживать технологию управления правами доступа к документам и сообщениям электронной почты, совместимую с ActiveDirectory.</li> <li>• Возможность поддержки открытых форматов OpenOffice XML (без промежуточной конвертации) и OpenDocument (непосредственно или с помощью дополнительных программных модулей).</li> <li>• Все приложения пакета локализованы на русский язык.</li> <li>• Возможность использовать многоязычный пользовательский интерфейс (включая русский и английский языки) с возможностью переключения между языками в процессе работы.</li> <li>• Пакет стандартных клиентских лицензии для рабочих станций для доступа к имеющимся в инфраструктуре заказчика серверам: <ul style="list-style-type: none"> <li>• серверу обеспечения доменной инфраструктуры ActiveDirectory,</li> <li>• серверу обмена сообщениями электронной почты, управлению задачами, календарями и совместной работы, совместимого с сервером</li> <li>• серверу платформы внутреннего портала, совместной работы, автоматизации бизнес-процессов и представления данных</li> <li>• серверу обмена мгновенными сообщениями, уведомления о присутствии двусторонней видео и голосовой связи</li> <li>• серверу централизованного управления программным обеспечением на рабочих станциях (включая установку, обновление, инвентаризацию).</li> </ul> </li> </ul>
2	Дог. №385/29-еп/223-ФЗ от 26.06.2017	Предоставление неэксклюзивных имущественных прав на использование программного обеспечения «Антиплагиат» на один год
3	Контракт №69-АЭФ/223-ФЗ от 11.09.2017	<p>Комплект антивирусного программного обеспечения (продление прав пользования):</p> <hr/> <p>Антивирусная защита физических рабочих станций и серверов: Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License</p> <hr/> <p>Защита почтового сервера от спама: Kaspersky Anti-Spam для</p>

		Linux Russian Edition. 5000+ MailBox 1 year EducationalRenewal License
--	--	---

### 8.3 Перечень информационных справочных систем:

1. ЭБС Издательства «Лань» <http://e.lanbook.com/> ООО Издательство «Лань». Договор № 99 от 30 ноября 2017 г. Срок действия документа – с 01.01.18 по 31.12.18.

2. ЭБС «Университетская библиотека онлайн» [www.biblioclub.ru](http://www.biblioclub.ru) ООО «Директ-Медиа» Договор № 0811/2017/3 от 08 ноября 2017 г. Срок действия документа – с 01.01.18 по 31.12.18.

3. ЭБС «Юрайт» <http://www.biblio-online.ru> ООО Электронное издательство «Юрайт» Договор №0811/2017/2 от 08 ноября 2017 г. Срок действия документа – с 20.01.2018 по 19.01.2019.

4. ЭБС «BOOK.ru» <https://www.book.ru> ООО «КноРус медиа» Договор № 61/223-ФЗ от 09 января 2017 г. Срок действия документа – с 09.01.2018 по 31.12.2018.

5. ЭБС «ZNANIUM.COM» [www.znanium.com](http://www.znanium.com) ООО «ЗНАНИУМ» Договор № 1812/2017 от 18 декабря 2017 г. Срок действия документа – с 01.01.18 по 31.12.18.

### 9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащённость
1.	Лекционные занятия	<p>Аудитория 7, оснащённая учебной мебелью, интерактивной доской, проектором, колонками, микрофоном, портретами и фотографиями классиков и современных представителей юридической науки; наборами демонстрационного оборудования и учебно-наглядными пособиями.</p> <p>Аудитория 9, оснащённая учебной мебелью, доской для демонстрации учебного материала, микрофоном, колонками для работы микрофона, наборами демонстрационного оборудования и учебно-наглядными пособиями.</p> <p>Аудитория 10, оснащённая учебной мебелью, интерактивной доской, проектором, микрофоном, колонками для работы микрофона, плакатом с латинскими высказываниями, переведенными на русский язык, флагом РФ, портретами классиков юридической науки, наборами демонстрационного оборудования и учебно-наглядными пособиями.</p> <p>Аудитория 17, оснащённая учебной мебелью, техническими средствами обучения, интерактивной доской, проектором, наборами демонстрационного оборудования и учебно-наглядными пособиями, картой РФ, картой субъектов РФ, гимном РФ, гимном Краснодарского края, гербом Краснодарского края, флагом Краснодарского края, плакатом со знаменательными датами истории Краснодарского края, картой Краснодарского края и Республики Адыгея, портретами и</p>

		<p>фотографиями классиков и современных представителей юридической науки.</p> <p>Аудитория 18, оснащённая учебной мебелью, техническими средствами обучения, интерактивной доской, проектором, микрофоном, наборами демонстрационного оборудования и учебно-наглядными пособиями, портретами классиков юридической науки, плакатом с историческими картами; плакатом с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 406, оснащённая интерактивной доской, проектором, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 01, оснащённая интерактивной доской, проектором, учебной мебелью, портретами классиков юридической науки, учебно-наглядными пособиями.</p> <p>Аудитория 02, оснащённая интерактивной доской, проектором, учебной мебелью, портретами классиков юридической науки, учебно-наглядными пособиями.</p>
2.	Семинарские занятия	<p>Аудитория 3, оснащённая доской, учебной мебелью.</p> <p>Аудитория 5, оснащённая доской для демонстрации учебного материала, стендом с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 13 (центр деловых игр), оснащённая мебелью, техническими средствами обучения, позволяющими проводить деловые игры двумя и более командами.</p> <p>Аудитория 105, оснащённая учебной мебелью, техническими средствами обучения.</p> <p>Аудитория 106, оснащённая учебной мебелью, техническими средствами обучения, проектором, учебно-наглядными пособиями.</p> <p>Аудитория 107, оснащённая доской, учебной мебелью.</p> <p>Аудитория 204, оснащённая доской, учебной мебелью.</p> <p>Аудитория 205, оснащённая доской, учебной мебелью, учебно-наглядными пособиями, манекенами для сердечно-легочной реанимации, носилками, аптечкой первой помощи.</p> <p>Аудитория 208, оснащённая доской, учебной мебелью, портретами ученых-юристов.</p> <p>Аудитория 209, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 304, оснащённая доской, учебной мебелью, портретами и фотографиями классиков юридической науки, учебно-наглядными пособиями и плакатами с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 305, оснащённая доской, учебной мебелью, учебно-наглядными пособиями и плакатами с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 306, оснащённая доской, учебной мебелью, учебно-наглядными пособиями и плакатами с латинскими</p>

		<p>высказываниями, переведенными на русский язык.</p> <p>Аудитория 307, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 308, оснащённая доской, учебной мебелью, настенной картой, шкафами с литературой, телевизором, принтером и сканером.</p> <p>Аудитория 404, оснащённая доской, учебной мебелью, портретами классиков юридической науки, учебно-наглядными пособиями.</p> <p>Аудитория 405, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 407, оснащённая доской, учебной мебелью, портретами классиков юридической науки.</p> <p>Аудитория 002, оснащённая доской, учебной мебелью.</p> <p>Аудитория 003, оснащённая доской, учебной мебелью.</p> <p>Аудитория 03, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 03А, оснащённая доской, учебной мебелью.</p> <p>Аудитория 06, оснащённая доской, учебной мебелью.</p> <p>Аудитория 08, оснащённая доской, учебной мебелью.</p> <p>Аудитория 09, оснащённая доской, учебной мебелью.</p> <p>Аудитория 010, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 012, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p>
3.	Лабораторные занятия	не предусмотрены
4.	Курсовое проектирование	Библиотека; кабинеты для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченные доступом в электронную информационно-образовательную среду университета; методические кабинеты кафедры уголовного права и криминологии (ауд. 103, 201, 302, 303, 311, 011).
5.	Групповые (индивидуальные) консультации	Аудитория 303, оснащённая мебелью, в том числе шкафами с литературой, телевизором, дипломами на стенах, свидетельствующими о достижениях членов кафедры.
6.	Текущий контроль, промежуточная аттестация	<p>Аудитория 3, оснащённая доской, учебной мебелью.</p> <p>Аудитория 5, оснащённая доской для демонстрации учебного материала, стендом с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 13 (центр деловых игр), оснащённая мебелью, техническими средствами обучения, позволяющими проводить деловые игры двумя и более командами.</p> <p>Аудитория 105, оснащённая учебной мебелью, техническими средствами обучения.</p> <p>Аудитория 106, оснащённая учебной мебелью, техническими средствами обучения, проектором, учебно-наглядными пособиями.</p> <p>Аудитория 107, оснащённая доской, учебной мебелью.</p>

		<p>Аудитория 204, оснащённая доской, учебной мебелью.</p> <p>Аудитория 205, оснащённая доской, учебной мебелью, учебно-наглядными пособиями, манекенами для сердечно-легочной реанимации, носилками, аптечкой первой помощи.</p> <p>Аудитория 208, оснащённая доской, учебной мебелью, портретами ученых-юристов.</p> <p>Аудитория 209, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 304, оснащённая доской, учебной мебелью, портретами и фотографиями классиков юридической науки, учебно-наглядными пособиями и плакатами с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 305, оснащённая доской, учебной мебелью, учебно-наглядными пособиями и плакатами с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 306, оснащённая доской, учебной мебелью, учебно-наглядными пособиями и плакатами с латинскими высказываниями, переведенными на русский язык.</p> <p>Аудитория 307, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 308, оснащённая доской, учебной мебелью, настенной картой, шкафами с литературой, телевизором, принтером и сканером.</p> <p>Аудитория 404, оснащённая доской, учебной мебелью, портретами классиков юридической науки, учебно-наглядными пособиями.</p> <p>Аудитория 405, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 407, оснащённая доской, учебной мебелью, портретами классиков юридической науки.</p> <p>Аудитория 002, оснащённая доской, учебной мебелью.</p> <p>Аудитория 003, оснащённая доской, учебной мебелью.</p> <p>Аудитория 03, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 03А, оснащённая доской, учебной мебелью.</p> <p>Аудитория 06, оснащённая доской, учебной мебелью.</p> <p>Аудитория 08, оснащённая доской, учебной мебелью.</p> <p>Аудитория 09, оснащённая доской, учебной мебелью.</p> <p>Аудитория 010, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p> <p>Аудитория 012, оснащённая доской, учебной мебелью, учебно-наглядными пособиями.</p>
7.	Самостоятельная работа	<p>Библиотека; кабинеты для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченные доступом в электронную информационно-образовательную среду университета; методические кабинеты кафедры уголовного права и криминологии (ауд. 103, 201, 302, 303, 311, 011).</p>

8.	Зал для проведения учебных судебных заседаний	Аудитория 12, оснащенная специальной мебелью и судебной атрибутикой.
----	---	--