МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное образовательное учреждение

высшего профессионального образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Филиал в г. Избербаше

Кафедра юридических дисциплин

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Преступления в сфере информационных технологий»

по направлению **40.03.01 (030900.62) «Юриспруденция»**

Профиль подготовки
Уголовное право

Уровень высшего образования
Бакалавриат

Форма обучения
Очная, заочная

Статус дисциплины
Базовая

Избербаш 2014

Рабочая программа дисциплины «**Преступления в сфере информационных технологий**» разработана в 2014 году в соответствии с требованиями ФГОС ВО по направлению подготовки **40.03.01 (030900.62) Юриспруденция** профиль подготовки «Уголовное право», утверждённого приказом Министерства образования и науки Российской Федерации от 21 декабря 2009 года № 747

Разработчик: Гитинова М.М., кандидат юридических наук

Рабочая программа дисциплины одобрена на заседании кафедры юридических дисциплин №05-10-14 от «7» октября 2014 г

Зав. кафедрой _____ Таилова А.Г.

(подпись)

Рабочая программа дисциплины утверждена на заседании Учебно-методической комиссии филиала от 21 октября 2014 г., протокол №1.

Председатель _____ Магомедов А.А.

(подпись)

СОДЕРЖАНИЕ

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

1.1. Цели и задачи дисциплины «Преступления в сфере информационных технологий»

Целью изучения дисциплины «**Преступления в сфере информационных технологий**» является реализация требований к освоению соответствующих компонентов профессиональных компетенций ПК-2, ПК-3, ПК-9 на основе формирования у студентов теоретических знаний в области **уголовного права, и отдельно - Преступлений в сфере информационных технологий,** а также получение навыков использования полученных знаний в профессиональной деятельности.

Задачи освоения учебной дисциплины заключаются в усвоении студентами теоретических знаний при изучении курса «**Уголовное право**», закрепления знаний о главе 28 УК РФ «**Преступления в сфере компьютерной информации».**

1.2. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «**Преступления в сфере информационных технологий**» студент должен обладать следующими общекультурными и профессиональными (ПК) компетенциями:

- имеет нетерпимое отношение к коррупционному поведению, уважительно относится к праву и закону (ОК-6);
- стремится к саморазвитию, повышению своей квалификации и мастерства (ОК-7);
- способен участвовать в разработке нормативно-правовых актов в соответствии с профилем своей профессиональной деятельности (ПК-1);
- способен осуществлять профессиональную деятельность на основе развитого правосознания, правового мышления и правовой культуры (ПК-2);
- способен принимать решения и совершать юридические действия в точном соответствии с законом (ПК-4);
- владеет навыками подготовки юридических документов (ПК-7); способен применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности (ПК-5);
- способен юридически правильно квалифицировать факты и обстоятельства (ПК-6);
- способен правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации (ПК-13);

В результате изучения дисциплины студент должен:

знать:

-понятие преступлений в сфере информационных технологий;

-уголовно-правовой анализ преступлений в сфере информационных технологий;

-дать криминологический анализ понятия «киберпреступность»;

- правового компонента их профессиональной подготовки,

- причины преступности в сфере информационных технологий, методах борьбы ней и субъектах ее осуществляющих данную борьбу.

уметь:

- оценивать события и явления общественной жизни с позиций закона и действовать в соответствии с его нормами;

- воспитать высокую правовую и нравственную культуру, уважение к правам и свободам граждан, добросовестное отношение к выполнению служебного и общественного долга в информационной сфере;

- анализировать материалы о составе осужденных, совершающих преступления в сфере информационных технологий,

- давать их социально-демографическую и уголовно-исполнительную характеристику;

- применять теоретические знания о преступлениях и преступности в сфере информационных технологий по российскому законодательству.

2. Указание места дисциплины в структуре образовательной программы

Учебная дисциплина «Преступления в сфере информационных технологий» нашла отражение в ООП по направлению подготовки 030900 юриспруденция (квалификация (степень) "бакалавр")
- дисциплины по выбору студента.
Для изучения учебной дисциплины «**Преступления в сфере информационных технологий**» необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Уголовное право», «Криминология», «Правовая статистика», «Уголовно-процессуальное право».

3. Объем дисциплины в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

ООП	Код дис-ны по УП	Трудоем-кость		Аудиторные часы					Самост. работа (часы)	Экза-мен (часы)
		ЗЕТ	часы	всего	из них:					
					лекц	ПЗ	курс. раб.	зачет		
очная форма обучения										
Проблемы института судимости		2	106	72	18	16	-	-	34	
заочная форма обучения										
Проблемы института судимости					8					

Примечание:

1.«*» в числителе указываются часы традиционных занятий, в знаменателе –интерактивных занятий.

4.Содержание дисциплины, структурированное по темам с указанием часов и видов учебных занятий

4.1 Тематический план для студентов очной формы обучения

№ п/п	Наименование разделов и тем	Общее кол-во часов	Аудиторные часы			Самостоя-тельная работа
			Всего	Лекции	Семинарские, практические. занятия	
1.	Информационное обеспечение борьбы с преступлениями в области информационныхтехнологий.	8	4	2	2	4
2	Уголовно-правовая характеристика преступлений в сфере компьютерной информации	8	4	2*	2	4
2	Понятие и отличительные особенности киберпреступности	8	4	2*	2	4
3.	Мошенничество в сфере компьютерной информации 159.6.УК РФ	8	4	2	2	4
4.	Криминалистическая характеристика компьютерных преступлений	8	4	2*	2*	4
5.	Современная уголовная политика в сфере борьбы с компьютерными преступлениями	8	4	2*	2	4
6	Криминалистические и иные (междисциплинарные) средства противодействия преступлениям в	8	4	2*	2	4

	сфере экономической деятельности с использованием современных информационных технологий.					
7	Меры предупреждения экономических преступлений, осуществляемые работниками служб безопасности	8	4	2	2	4
8	Обеспечение информационной безопасности детей в сети интернет	4	2	2		2
Итого:			68	18	16	34

Примечание:

Знаком /*/ выделены темы, по которым проводятся активные и интерактивные формы занят

4.2 Тематический план для студентов заочной формы обучения

№ п/п	Наименование разделов и тем	Общее к-во часов	Аудиторные часы			Самостоя-тельная работа
			Всего	Лекции	Семинарские, практические. занятия	
1	2	3	4	5	6	7
1.	Информационное обеспечени борьбы с преступлениями в области информационныхтехнологий			2		
2.	Уголовно-правовая характеристика преступлений в сфере компьютерной информации			2		
3	Понятие и отличительные особенности киберпреступности			2*		
4.	Мошенничество в сфере компьютерной информации			2*		

	159.6.УК РФ					
Итого:				8		

Примечание

Знаком /*/ выделены темы, по которым проводятся активные и интерактивные формы занятий.

Тема 1. Информационное обеспечение борьбы с преступлениями в области информационных технологий. Информационное обеспечение борьбы с преступлениями, связанными с подделкой документов. Информационное обеспечение международного розыска лиц. Общие положения.

Тема 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

Ст. 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Анализ объективных и субъективных признаков.

Тема 3. Понятие и отличительные особенности киберпреступности

Кибертерроризм в России: его свойства и особенности. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности. Кибертерроризм- как реальная угроза внешнему и внутреннему контурам национальной безопасности России. Ответственность за киберпреступления. Зарубежная практика по

формированию борьбы с кибермошенничеством. Российская практика противодействия кибермошенничеству.

Тема 4. Мошенничество в сфере компьютерной информации (статья 159.6. УК РФ).

Общая характеристика преступления ст. 159.6 УК РФ. Уголовно-правовой анализ. Выделение объекта, объективной стороны, субъекта, субъективной стороны. Проблемы квалификации. Анализ правоприменения. Криминологическая характеристика лиц, совершающих деяния, предусмотренные статьей 159.6 УК РФ. Риски недостаточного обеспечения информационной безопасности

Тема 5. Криминалистическая характеристика компьютерных преступлений .

Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК РФ. Высокая латентность указанных преступлений и причины. Сложность сбора доказательств и процесса доказывания. Широкий спектр криминалистически значимых признаков преступлений. Отсутствие единой программы борьбы с киберпреступлениями. Сложность расследования и раскрытия компьютерных преступлений. Отсутствие обобщенной судебной и следственной практики по делам данной категории. Нехватка высокопрофессиональных специалистов, представителей правоохранительных органов.

Тема6. Современная уголовная политика в сфере борьбы с компьютерными преступлениями

Понятие и многоаспектность компьютерных преступлений. Наиболее распространенные преступления, совершаемые с использованием компьютерной техники: хакерство, компьютерное мошенничество, распространение вредоносных программ, компьютерное пиратство. Цели и

задачи уголовной политики в сфере противодействия компьютерной преступности. Правовая основа противодействия компьютерной преступности.

Тема 7. Криминалистические и иные (междисциплинарные) средства противодействия преступлениям в сфере экономической деятельности с использованием современных информационных технологий. Программы обеспечения информационной безопасности. Проблемы защиты объектов собственности в том числе и интеллектуальной в сфере экономической деятельности.

Тема 8. Меры предупреждения экономических преступлений, осуществляемые работниками служб безопасности

Основные задачи службы экономической безопасности. Функции экономической безопасности. Направления деятельности служб безопасности. Систематическая информационно-аналитическая работа для установления приемов и способов хищений на предприятиях; категории лиц, наиболее часто совершающие хищения; обстоятельства, способствующие совершению преступлений; наиболее эффективные меры перекрытия лазеек для совершения хищения и другие вопросы.

4.3. Планы семинарских занятий

Тема 1. Информационное обеспечение борьбы с преступлениями в области информационных технологий.

Вопросы к обсуждению:

1. Преступность в сфере информационных технологий: тенденции и перспективы
2. Информационное обеспечение борьбы с преступлениями, связанными с подделкой документов.
3. Информационное обеспечение международного розыска лиц. Общие положения.

Тема 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

Вопросы к обсуждению:

1. Ст. 272. Неправомерный доступ к компьютерной информации
2. Статья 273. Создание, использование и распространение вредоносных компьютерных программ. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
3. Анализ объективных и субъективных признаков.

Тема 3*. Понятие и отличительные особенности киберпреступности

Вопросы к обсуждению:

1. Кибертерроризм в России: его свойства и особенности.
2. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности.
3. Кибертерроризм- как реальная угроза внешнему и внутреннему контурам национальной безопасности России.
4. Ответственность за киберпреступления. Зарубежная практика по формированию борьбы с кибермошенничеством.

5. Российская практика противодействия кибермошенничеству.

Тема 4. Мошенничество в сфере компьютерной информации (статья 159.6. УК РФ).

Вопросы к обсуждению:

1. Характеристика преступления ст. 159.6 УК РФ. Уголовно-правовой анализ.
2. Проблемы квалификации.
3. Анализ правоприменения.
4. Криминологическая характеристика лиц, совершающих деяния, предусмотренные статьей 159.6 УК РФ.
5. Риски недостаточного обеспечения информационной безопасности

Семинар № 5*

Тема: Криминалистическая характеристика компьютерных преступлений .

Вопросы к обсуждению:

1. Проблемы криминалистической тактики при расследовании преступлений, предусмотренных главой 28 УК РФ.
2. Высокая латентность указанных преступлений и причины.
3. Сложность сбора доказательств и процесса доказывания.
4. Сложность расследования и раскрытия компьютерных преступлений.
5. Отсутствие обобщенной судебной и следственной практики по делам данной категории.

Семинар № 6*

Тема: Современная уголовная политика в сфере борьбы с компьютерными преступлениями

Вопросы к обсуждению:

1. Понятие и многоаспектность компьютерных преступлений.
2. Наиболее распространенные преступления, совершаемые с использованием компьютерной техники: хакерство, компьютерное мошенничество, распространение вредоносных программ, компьютерное пиратство.
3. Цели и задачи уголовной политики в сфере противодействия компьютерной преступности.
4. Правовая основа противодействия компьютерной преступности.

Практическое занятие № 7*

Тема 7. Криминалистические и иные (междисциплинарные) средства противодействия преступлениям в сфере экономической деятельности с использованием современных информационных технологий.

Вопросы к обсуждению:

1. Программы обеспечения информационной безопасности.
2. Проблемы защиты объектов собственности в том числе и интеллектуальной в сфере экономической деятельности.

Семинар № 8

Тема 8. Меры предупреждения экономических преступлений, осуществляемые работниками служб безопасности.

Вопросы к обсуждению:

1. Основные задачи службы экономической безопасности.
2. Функции экономической безопасности.
3. Направления деятельности служб безопасности.
4. Систематическая информационно-аналитическая работа для установления приемов и способов хищений на предприятиях; категории лиц, наиболее часто совершающие хищения; обстоятельства, способствующие совершению преступлений; наиболее эффективные меры перекрытия лазеек для совершения хищения и другие вопросы.

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

Время, выделенное учебным планом на освоение образовательной дисциплины, отводится на аудиторные формы работы (лекционные и семинарские занятия, другие виды аудиторных занятий), которые проводятся при непосредственном участии преподавателя. Вторая часть установленных стандартом часов отводится для самостоятельной, или внеаудиторной, работы студентов.

Под самостоятельной работой студентов понимается планируемая учебная, учебно-исследовательская, а также научно-исследовательская работа студентов, которая выполняется во внеаудиторное время по инициативе студента или по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Виды самостоятельной работы студентов

Основными видами самостоятельной учебной деятельности студентов высшего учебного заведения являются:

1) предварительная подготовка к аудиторным занятиям, в том числе и к тем, на которых будет изучаться новый, незнакомый материал. Такая подготовка предполагает изучение рабочей программы, установление связи с ранее полученными знаниями, выделение наиболее значимых и актуальных проблем, на изучении которых следует обратить особое внимание и др.;

2) самостоятельная работа при прослушивании лекций, осмысление учебной информации, сообщаемой преподавателем, ее обобщение и краткая запись, а также своевременная доработка конспектов лекций;

3) подбор, изучение, анализ и при необходимости – конспектирование рекомендованных источников по учебным дисциплинам;

4) выяснение наиболее сложных, непонятных вопросов и их уточнение во время консультаций;

5) подготовка к контрольным занятиям, зачетам и экзаменам;

6) выполнение специальных учебных заданий, предусмотренных рабочей программой;

7) написание рефератов, контрольных, курсовых, квалификационных, дипломных работ и их защита;

8) выполнение собственных научных исследований, участие в научных исследованиях, проводимых в масштабе кафедры, факультета, института и университета в целом;

9) производственная практика по приобретаемой в университете специальности;

10) систематическое изучение периодической печати, научных монографий, поиск и анализ

Оценка самостоятельной работы студентов

Отдельной составляющей в итоговой оценке по предмету является оценка самостоятельной работы студента.

Во-первых, оценка самостоятельной работы включается в оценку такой формы промежуточного контроля, как оценка текущей работы на семинарских занятиях.

Во-вторых, так как самостоятельная работа по предмету поощряется, преподаватель может использовать (и, как правило, использует) оценку самостоятельной работы в качестве поощрительной составляющей на экзамене.

В спорных ситуациях оценка самостоятельной работы может разрешить ситуацию в пользу студента.

Независимо от вида самостоятельной работы, показателями самостоятельной работы могут считаться:

а) умение проводить анализ;

б) умение выделить главное (в том числе, умение ранжировать проблемы);

в) самостоятельность в поиске и изучении статистических источников, т.е. способность обобщать материал не только из лекций, но и из разных прочитанных и изученных источников и из жизни;

г) положительное собственное отношение, заинтересованность в предмете;

д) умение применять свои знания для ответа на вопросы.

Методическое обеспечение самостоятельной работы осуществляется на основе открытого доступа студентов к учебно-методическим ресурсам института, а также предоставления обучающимся списков обязательной и дополнительной литературы.

6. Фонд оценочных средств для проведения промежуточной аттестации, обучающихся по дисциплине

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

№	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Информационное обеспечение борьбы с преступлениями в области информационныхтехнологи	ОК–5,ПК-2	Коллоквиум, Презентация Доклад
2.	Уголовно-правовая характеристика преступлений в сфере компьютерной информации	ПК-2,ПК-3	Коллоквиум, тестирование
3.	Понятие и отличительные особенности киберпреступности	ОК–5, ПК-2,ПК-3	Коллоквиум, тестирование
4.	Мошенничество в сфере компьютерной информации 159.6.УК РФ	ПК-2, ПК-3	Контрольная работа
5.	Криминалистическая характеристика компьютерных преступлений	ОК–5; ПК-2,ПК-3	Коллоквиум, тестирование Презентация-доклад
6.	Современная уголовная политика в сфере борьбы с компьютерными преступлениями	ПК-3, ПК-9	Коллоквиум, тестирование
7.	Криминалистические и иные (междисциплинарные) средства противодействия преступлениям в сфере экономической деятельности с использованием	ПК-2,ПК-3,ПК-9	Коллоквиум, тестирование

	современных информационных технологий.		
8.	Меры предупреждения экономических преступлений, осуществляемые работниками служб безопасности	ПК-2,ПК-3	коллоквиум, тестирование
9.	Обеспечение информационной безопасности детей в сети интернет	ПК-2,ПК-3,ПК-9	Контрольная работа

* Наименование темы (раздела) или тем (разделов) берется из рабочей программы дисциплины.

6.2. Описание показателей и критериев оценивания компетенций

Перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3	4
1	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы темам/разделам дисциплины
2	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий
3	Доклад,сообщение	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения	Темы докладов, сообщений

		определенной учебно-практической, учебно-исследовательской или научной темы	
4	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
5	Презентация-доклад	Наглядность Репрезентативность Доступность Убедительность Наличие фактов	

Критерии оценки:

-оценка **«отлично»** выставляется студенту, если ответ аргументирован, обоснован и дана самостоятельная оценка изученного материала;

- оценка **«хорошо»** ставится студенту, если ответ аргументирован, последователен, но допущены некоторые неточности;

- оценка **«удовлетворительно»** ставится студенту, если ответ является неполным и имеет существенные логические несоответствия;

- оценка **«неудовлетворительно»** если в ответе отсутствует аргументация, тема не раскрыта.

6.3.2. Вопросы для коллоквиумов, круглых столов

1. Международное законодательство и законодательство России в области борьбы с правонарушениями и преступлениями в сфере информационныхтехнологий

2. Законодательство зарубежных государств в области борьбы с правонарушениями и преступлениями в сфере информационныхтехнологий

3. Система международных органов, государственных органов России и зарубежных государств, осуществляющих борьбу с преступлениями в сфере информационныхтехнологий.

4. Криминологическая характеристика преступлений в сфере экономики и информационныхтехнологий
5. Актуальные вопросы предупреждения и противодействия преступлениям в сфере информационныхтехнологий

Критерии оценки:

оценка «отлично» выставляется студенту, если ответ аргументирован, обоснован и дана самостоятельная оценка изученного материала;

- оценка «хорошо» ставится студенту, если ответ аргументирован, последователен, но допущены некоторые неточности;
- оценка «удовлетворительно» ставится студенту, если ответ является неполным и имеет существенные логические несоответствия;

оценка «неудовлетворительно», если в ответе отсутствует аргументация, тема не раскрыта.

6.3.3.Примерная тематика письменных (контрольных) работ

1. Понятие преступлений и правонарушений в сфере информационных технологий.
2. Факторы роста преступлений и правонарушений в сфере информационныхтехнологий.
3. Нормы о каких правонарушениях были рекомендованы к включению в национальное законодательство Рекомендацией R№ 89 “О компьютерной преступности”.
4. Какие правонарушения в соответствии с Конвенцией “О киберпреступности” относятся к компьютерным преступлениям.
5. Законодательство России регламентирующие ответственность за преступления и правонарушения в сфере информационныхтехнологий.
6. Понятие информационной безопасности РФ.
7. Соотношение доктрины информационной безопасности РФ и доктрины национальной безопасности РФ.
8. Основные составляющие национальных интересов России в информационной сфере.
9. Методы обеспечения информационной безопасности: понятие и общая характеристика (правовые, организационно-технические, экономические).
10. Какие преступления в соответствии с действующим уголовным кодексом РФ могут быть отнесены к преступлениям в сфере

информационныхтехнологий: понятие и общая характеристика.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ аргументирован, обоснован и дана самостоятельная оценка изученного материала;
- оценка «хорошо» ставится студенту, если ответ аргументирован, последователен, но допущены некоторые неточности;
- оценка «удовлетворительно» ставится студенту, если ответ является неполным и имеет существенные логические несоответствия;

оценка «неудовлетворительно» если в ответе отсутствует аргументация, тема не раскрыта.

6.3.3. Фонды оценочных средств

Темы (варианты) контрольных работ

1 вариант. Вопрос. Понятие преступлений и правонарушений в сфере высоких технологий.

Задача. Служащий банка «Южный» Игрунков приобрел на рынке компакт–диск с компьютерной игрой «Звездные войны II». На следующий день Игрунков установил игру на своем рабочем компьютере, связанном по сети с другими компьютерами банка. В результате распространения вируса, записанного на компакт–диске, компьютерная система банка была выведена из строя и не могла нормально функционировать более суток, из–за чего банк понес существенные убытки.

Как квсишфицироватъ действия Игрункова?

2 вариант. Вопрос. Причины и условия, место преступлений в сфере экономики и высоких технологий в общей доли преступности.

Задача. Студент Технического университета Артемов, Преодолев ради любопытства систему защиты коммерческого эротического вебсайта, распространил информацию о способе взлома системы защиты этого сайта в компьютерной сети. Там же он поместил информацию о зарегистрированных пользователях упомянутого сайта, включая сведения о номерах их кредитных карт. В последующие несколько часов сайт подвергся массированным атакам сетевых хулиганов со всего мира, в результате чего прекратил функционирование на несколько дней. Кроме того, нелегальным использованием кредитных карт был причинен ущерб их законным владельцам.

Дайте юридическую оценку действиям Артемова.

3 вариант. Вопрос. Классификация преступлений в сфере экономики и высоких технологий по кодификатору международной уголовной полиции генерального секретариата Интерпола.

Задача. Работник коммерческой организации «Окна» Воронин, не имеющий достаточного опыта работы на компьютере, случайно удалил из памяти главного компьютера организации информацию о ее новых разработках, из–за чего эта организация понесла значительные убытки. По заявлению директора в отношении Воронина было возбуждено уголовное дело по признакам ч. 2 ст. 274 УК. Однако Воронин заявил следователю, что никаких правил работы на компьютере руководство организации не утверждало, и потому он не должен подлежать уголовной ответственности.

Верны ли доводы Воронина?

4 вариант. Вопрос. Основные направления профилактики преступлений в сфере экономики и высоких технологий.

Задача. Компьютерный энтузиаст Доменов, придерживаясь определенных политических взглядов, в разгар предвыборной кампании проник в один из «серверов имен» глобальной сети интернет и подменил сетевой адрес вебсайта партии «Яблоко» на адрес вебсайта КПРФ, из–за чего все пользователи сети, запрашивающие новости партии «Яблоко», попадали на агитационную страницу КПРФ.

Как квалифицировать действия Доменова?

Тесты :

1. **Задание** В хартии глобального информационного общества отмечается, что ….. технологии вошли в число наиболее существенных факторов, влияющих на формирование современного общества.
2. **Задание** По действующему российскому законодательству, такие деяния, подпадают под сферу действия различных нормативных актов:

☐ Уголовный кодекс РФ
☐ Гражданском кодекс РФ
☐ Об участии в международном информационном обмене
☐ О правовой охране программ для электронных вычислительных машин и баз данных
☐ Концепция национальной безопасности
☐ Доктрина информационной безопасности Российской Федерации
☐ КОАП РФ

3. **Задание** Какая глава Уголовного кодекса РФ регламентирует уголовную ответственность за совершение преступлений в сфере экономики и высоких технологий – ….
4. **Задание** Какие деяния по действующему уголовному законодательству признаются преступными:

☐ Неправомерный доступ к компьютерной информации
☐ Умышленное блокирование или уничтожение компьютерной информации

☐ Создание, использование и распространение вредоносных программ для ЭВМ
☐ Компьютерное мошенничество
☐ Нарушение правил эксплуатации ЭВМ, их системы или сети

5. **Задание** Термин «Преступления в сфере экономики и высоких технологий» является относительно новым и дискуссионным для российской уголовно–правовой действительности, при этом дискуссии, идут в следующих направлениях:

☐ критерии отнесения общественно–опасных деяний к группе так называемых «компьютерных преступлений»;
☐ ставиться под сомнение целесообразности использования термина «компьютерные преступления» с предложениями взамен – «информационные преступления», «Преступления в сфере экономики и высоких технологий» (как разновидность – преступления в сфере информации), «киберпреступления» и т.д.
☐ как рассматривать современные высокие технологии, которые использовались при совершении преступления – как орудие совершения или как особый способ совершения преступления

6. **Задание** Преступления в сфере экономики и высоких технологий – это умышленные деяния, причиняющие вред охраняемым уголовным законом общественным отношениями и совершенные лицом с использованием современных высоких технологий, в том числе и компьютерной техники.

7. **Задание** Принято выделять два типа причинного комплекса преступлений в сфере экономики и высоких технологий:

☐ Причинный комплекс, не имеющий особенностей по сравнению с другими, «некомпьютерными» видами преступности. Отличие заключается только в том, что преступники дополнительно используют компьютерные технологии. В результате несколько изменяются условия преступной деятельности, ее формы, масштабы и последствия.
☐ Причинный комплекс который заключается в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений. связанных с появлением автоматизированных систем обработки информации.
☐ Причинный комплекс связанный с повсеместное и всестороннее внедрение новых технологий привело к техническому оснащению отдельных преступников и организованных преступных групп.

8. **Задание** Прогнозирование ситуации показывает, что в российских условиях рост преступлений в сфере экономики и высоких технологий, обусловлен следующими факторами:

☐ рост числа ЭВМ, используемых в России и, как следствие этого, ростом числа их пользователей, увеличением объемов информации, хранимой в ЭВМ;

☐ недостаточностью защиты программного обеспечения;
☐ непродуманной кадровой политикой в вопросах приема на работу и увольнения;
☐ отсутствием законодательной базы.

9. **Задание** Рассматриваемые преступления характеризуется очень высокой …. . Так, по оценкам специалистов, нераскрытыми остаются 85% дел, возбужденных по признакам данных преступных деяний.

10. **Задание** Какие из ниже перечисленных нормативных актов относятся к международному законодательству в области борьбы с правонарушениями и преступлениями в сфере высоких технологий:

☐ Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г
☐ «Конвенция о киберпреступности» принятая Советом Европы 9 ноября 2001 г. в Страсбурге.
☐ Кодификатор международной уголовной полиции генерального секретариата Интерпола.

11. **Задание** Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, к рекомендуемому перечню преступлений относит.

☐ Компьютерное мошенничество
☐ Компьютерный подлог
☐ Причинение ущерба компьютерным данным или компьютерным программам
☐ Компьютерный саботаж
☐ Несанкционированный доступ
☐ Несанкционированный перехват
☐ Несанкционированное воспроизведение охраняемой авторским правом компьютерной программы
☐ Несанкционированное воспроизведение микросхемы
☐ Распространение детской порнографии посредством сети Интернет
☐ Несанкционированное использование охраняемой законом компьютерной программы

12. **Задание** Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, к факультативному перечню преступлений относит.

☐ Неправомерное изменение компьютерных данных или компьютерных программ
☐ Компьютерный шпионаж
☐ Несанкционированный перехват
☐ Несанкционированное воспроизведение охраняемой авторским правом компьютерной программы
☐ Несанкционированное использование компьютера

☐ Несанкционированное использование охраняемой законом компьютерной программы

13. **Задание** Содержит ли Конвенция положения о корпоративной ответственности (принятие мер, какие могут быть необходимы для обеспечения возможности привлечения юридических лиц к ответственности за уголовное преступление):

☐ Да, в целях обеспечения возможности привлечения юридических лиц к ответственности за уголовное преступление, которое совершается в его пользу любым физическим лицом;

☐ Нет, так как ответственность юридических лиц по уголовному законодательству не возможна.

14. **Задание** Принятие Конвенции по борьбе с киберпреступностью позволило приблизить достижение следующих поставленных в ней целей:

☐ согласование государствами–участниками национальных уголовно–правовых норм, связанных с преступлениями в киберпространстве;

☐ разработка процедур процессуального законодательства, необходимых для расследования таких преступлений и судебного преследования лиц, их совершивших, а также сбора доказательств, находящихся в электронной форме;

☐ обеспечение быстрого и эффективного режима международного сотрудничества в данной области;

15. **Задание** Россия, помимо многочисленных договоров о правовой помощи, является участником ….. о сотрудничестве государств–участников СНГ в борьбе с преступлениями в сфере компьютерной информации.

16. **Задание** В соответствии со ст. 272 УК РФ уголовно наказуемым признается … доступ к охраняемой законом компьютерной информации

☐ несанкционированный
☐ преступный
☐ неправомерный
☐ злоумышленный
☐ неосторожный

17. **Задание** … информации – сведения на машинном носителе, в электронно–вычислительной машине (ЭВМ), системе ЭВМ или их сети

18. **Задание** Классификация преступлений в сфере экономики и высоких технологий по кодификатору международной уголовной полиции генерального секретариата Интерпола, в соответствии с названным кодификатором все компьютерные преступления классифицированы следующим образом:

☐ Несанкционированный доступ и перехват;
☐ компьютерный абордаж (несанкционированный доступ);
☐ Изменение компьютерных данных;
☐ Компьютерное мошенничество;

☐ мошенничество с банкоматами;
☐ Незаконное копирование;
☐ Компьютерный саботаж;
☐ передача информации, подлежащая судебному рассмотрению.

19. **Задание** Какой нормативный акт является основополагающим в сфере борьбы с преступлениями в сфере высоких технологий на территории России:

☐ Доктрина информационной безопасности Российской Федерации;
☐ Доктрина национальной безопасности Российской Федерации;
☐ Соглашение о сотрудничестве стран СНГ в борьбе с компьютерными преступлениями.

20. **Задание** Доктрина информационной безопасности Российской Федерации представляет собой совокупность …. взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

21. **Задание** Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в ……. сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

22. **Задание** Доктрина информационной безопасности Российской Федерации представляет служит основой для:

☐ формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
☐ подготовки предложений по совершенствованию правового, методического, научно – технического и организационного обеспечения информационной безопасности Российской Федерации;
☐ привлечения к уголовной ответственности лиц совершивших Преступления в сфере экономики и высоких технологий;
☐ разработки целевых программ обеспечения информационной безопасности Российской Федерации.

23. **Задание** Соответствие между видом угрозы информационной безопасности Российской Федерации и ее содержанием

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.	1. Вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи.
2. Угрозы информационному обеспечению государственной	2. Противодействие, в том числе со стороны криминальных структур,

политики Российской Федерации.	реализации гражданами своих прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений.
3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи.	3. Монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами, блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории.
4. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.	4. Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно – телекоммуникационных систем, в том числе систем защиты информации.

24.**Задание** Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние:

☐ деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
☐ неблагоприятная криминогенная обстановка;
☐ недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
☐ слабая правовая культура граждан;
☐ доступ физических лиц в мировое информационное пространство.

25.**Задание** Основные элементы организационной основы системы обеспечения информационной безопасности РФ:

☐ Президент РФ и органы исполнительной власти;
☐ Федеральное собрание РФ;
☐ Межведомственные и государственные комиссии;
☐ Органы судебной власти;
☐ Юридические лица;
☐ Граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности.

26. **Задание** С уголовно–правовой точки зрения, компьютерная сеть Интернет используется как инструмент пропаганды и организации, следующих преступных деяния направленных против общественных отношений в сфере общественной безопасности:

☐ преступления, предусмотренные статьями 205; 205.1; 205.2; 206; 208; 211; 277; 278; 279; 360 УК РФ;
☐ преступления предусмотренные статьями 213, 214 УК РФ;
☐ преступления, предусмотренные статьями 277; 278; 279; 360 УК РФ.

27. Задание Общественная опасность мошенничества с использованием банковских пластиковых карт определяется, характером ….. объектов посягательства, которыми являются собственность, законный оборот информации, отношения в сфере законного изготовления и оборота денежных средств.

28. Задание Предмет мошенничества с использованием банковских пластиковых карт, обладает:

☐ материальными признаками;
☐ информационными признаками;
☐ только материальными признаками;
☐ только информационным и признаками.

29. **Задание** …….. т.е оплата несуществующими картами, создание фальшивых виртуальных магазинов, электронное воровство, фальшивая оплата в игорных заведениях.

30. Задание Какие деяния признаются преступными в соответствии с уголовным законодательством зарубежных стран:

☐ уклонение от оплаты услуг в сфере телекоммуникаций;
☐ взятка за содействие незаконному перехвату или записи телекоммуникационных сообщений;
☐ нарушение конфиденциальности электронной почты и голосовых сообщений;
☐ ввод или хранение в памяти ЭВМ запрещенных законом данных;
☐ изготовление или владение компьютерными программами или аппаратами, специально предназначенными для совершения преступлений;
☐ незаконное получение доступа к персональным данным;
☐ установка не лицензионного программного обеспечения.

6.3.5.Перечень вопросов к итоговому контролю (зачету)

1. Формы сотрудничества стран СНГ в сфере борьбы с компьютерными преступлениями.
2. Выбор стратегии борьбы с преступлениями в сфере информационныхтехнологий: понятие и общая характеристика.
3. Условия успешности реализации выбранной стратегии (постоянная и планомерная работа, взаимодействие правоохранительных органов).
4. Общая характеристика системы правоохранительных США осуществляющих борьбу с компьютерными преступлениями.
5. Общая характеристика системы правоохранительных России осуществляющих борьбу с преступлениями в сфере информационныхтехнологий.
6. Какие отделы выделяются в системе правоохранительных зарубежных государств осуществляющих борьбу с компьютерными преступлениями.
7. Роль кадрового и технического обучения в деятельности правоохранительных органов России осуществляющих борьбу с преступлениями в сфере информационныхтехнологий.
8. Типовые модели разных категорий преступников совершающих преступлений в сфере экономики и информационныхтехнологий.
9. Аналитическая работа как средство предотвращения преступлений в сфере экономики и информационных технологий: понятие, цели, уровни.
10. Общая характеристика стратегического, тактического и оперативного анализа.
11. Основные направления профилактика и пресечение преступлений в сфере информационныхтехнология.

Материалы для проведения дискуссионного форума

ФОРУМ 1

1. Завладение или раскрытие коммерческой тайны с использованием электронных документов или информационных устройств.
2. Изготовление и распространение по телекоммуникационным сетям детской порнографии.
3. Использование или принуждение к использованию компьютерных систем для совершения преступлений против собственности.
4. Использование компьютерных технологий в целях извлечения прибыли путем создания финансовых «пирамид» и аналогичных махинаций.
5. Нарушение почтовой и телекоммуникационной тайны.

ФОРУМ 2

1. Проблемы квалификации мошенничества с использованием банковских пластиковых карт.
2. Раскрытие и распространение сообщений электронной почты, сведений

хранящихся в электронных базах данных.
3. Террористические акты, связанные с деяниями в области информатики.
4. Уголовная ответственность за нарушение свободы средств массовой информации.
5. Шантаж, вымогательство с угрозой уничтожения данных, сохраняемых в компьютере или компьютерной системе.

Критерии оценки:

Оценка **«зачтено»** выставляется студенту, который
- прочно усвоил предусмотренный программный материал;
- правильно, аргументировано ответил на все вопросы, с приведением примеров;
- показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов
- без ошибок выполнил практическое задание.

Обязательным условием выставленной оценки является правильная речь в быстром или умеренном темпе.

Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельной и контрольной работы, систематическая активная работа на семинарских занятиях.

2. Оценка **«не зачтено»** Выставляется студенту, который не справился с 50% вопросов и заданий билета, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем. Оценивается качество устной и письменной речи, как и при выставлении положительной оценки.

6.4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций.

Оценка знаний, умений, навыков, характеризующих этапы формирования компетенций по дисциплине «Финансы» осуществляется в ходе текущего и промежуточного контроля. Текущий контроль организуется в формах: устного опроса (беседы, индивидуального опроса, докладов); контрольных работ; проверка тестирования.

Промежуточный контроль осуществляется в формах зачета и итогового экзамена. Каждая форма промежуточного контроля должна включать в себя теоретические вопросы, позволяющие оценить уровень освоения студентами знаний и практические задания, выявляющие степень сформированности умений и навыков.

Процедура оценивания компетенций обучающихся основана на следующих принципах:
периодичности проведения оценки, многоступечатости оценки по устранению недостатков, единства используемой технологии для всех обучающихся, выполнения условий сопоставимости результатов оценивания, соблюдения последовательности проведения оценки.

Краткая характеристика процедуры реализации текущего и промежуточного контроля для оценки компетенций обучающихся включает:

доклад, сообщение_- продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Подготовка осуществляется во внеурочное время. На подготовку дается одна неделя. Результаты озвучиваются на втором занятии, регламент- 7 минут на выступление . В оценивании результата наравне с преподавателем принимают участие студенты группы.

устный опрос – устный опрос по основным терминам может проводиться в начале/конце лекционного или семинарского занятия в течении 15-20 мин. Либо устный опрос проводится в течение всего семинарского занятия по заранее выданной тематике.

тест – проводится на заключительном занятии. Позволяет оценить уровень знаний студентами теоретического материала по дисциплине. Осуществляется на бумажных носителей по вариантам. Количество вопросов в каждом варианте- 20. Отведенное время на подготовку – 60 мин.

зачет – проводится в заданный срок согласно графику учебного процесса. Зачет проходит в форме собеседования по вопросам. При итоговом контроле учитывается уровень приобретенных компетенций студента. Компонент «знать» оценивается теоретическими вопросами по содержанию дисциплины, компоненты «уметь» и «владеть» - практикоориентированными заданиями. Время принятия 10 минут-15 мин.

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

7.1.Нормативные правовые документы

1. Конституция РФ, 12 декабря 1993 г. Консультант плюс.
2. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 31.12.2014) (с изм. и доп., вступ. в силу с 23.01.2015).
3. Приказ МВД РФ N 786, Минюста РФ N 310, ФСБ РФ N 470, ФСО РФ N 454, ФСКН РФ N 333, ФТС РФ 971 от 06.10.2006 (ред. от 22.09.2009) "Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола" (Зарегистрировано в Минюсте РФ 03.11.2006 N 8437)

4. Постановление Правительства РФ от 29.06.1995 N 653 (ред. от 12.04.2010) "О заключении Соглашений о сотрудничестве между Министерством внутренних дел Российской Федерации и компетентными ведомствами иностранных государств".

5. "Комментарии законодательного регулирования оперативно-розыскной деятельности в Российской Федерации и за рубежом: Учебное пособие" (постатейный) (5-е издание, расширенное и переработанное) (Смирнов М.П.) (Подготовлен для системы КонсультантПлюс, 2012)

6. "Доктрина информационной безопасности Российской Федерации" (утв. Президентом РФ 09.09.2000 N Пр-1895).

7.2.Литература

Основная

7. Учебник уголовное право (особенная часть)
8. Криминология.
9. Криминалистика.
10. Комментарий к Уголовному кодексу Российской Федерации" (постатейный) (13-е издание, переработанное и дополненное) (отв. ред. В.М. Лебедев).- М.: Юрайт", 2013.

Дополнительная

11. Алгазин А.И., Галагуза Н.Ф., Ларичев В.Д. Страховое мошенничество и методы борьбы с ним: учебно-практическое пособие / под ред. В.Д. Ларичева. М.: Дело, 2003. 512 с.

12. Боровских Р.Н. Основы криминалистической характеристики преступлений в сфере страхования // Российский следователь. 2013. N 20. С. 27 - 35.

13. Гармаев Ю.П. Мультимедийные криминалистические и межотраслевые средства противодействия преступности: перспективы разработки и внедрения // Дружественное к ребенку правосудие и проблемы ювенальной уголовной политики: материалы IV международной научно-практической конференции (г. Улан-Удэ, 3 - 4 октября 2013 г.). Улан-Удэ: Изд-во БГУ. 2013. С. 43 - 48.

14. Ищенко Е.П., Водянова Н.Б. Алгоритмизация следственной деятельности: монография. М.: Юрлитинформ, 2010. 304 с.

15. Лопатина Т.М. Противодействие преступлениям в сфере компьютерной информации // Законность. 2006. N 6. С. 51.

16. Лубин С.А. Расследование преступлений в сфере страхования / Криминалистическое обеспечение экономической безопасности и борьбы с коррупцией: учебно-практическое пособие / под ред. А.Ф. Лубина и С.Ю. Журавлева. Н. Новгород: Нижегородская академия МВД России, 2012. 418 с.
17. Протасевич А.А., Зверянская Л.П.Криминалистическая характеристика компьютерных преступлений // Российский следователь", 2013, N 11.
18. Пучнин А.В. Особенности расследования экономических преступлений, связанных со служебной деятельностью: монография. М.: Юрлитинформ, 2013. 184 с.
19. Старостина Е. Кибертерроризм. URL: http://www.crimeresearch.ru/news/20.04.2005/1943/.
20. Тарасов А.М. Кибершпионы "Duqu", "Stuxnet", "Flame", "Gauss" - что дальше? // Право и кибербезопасность. 2012. N 1. С. 23 - 26.
21. Услинский Ф.А. Кибертерроризм в России: его свойства и особенности // Право и кибербезопасность", 2014, N 1.
22. Шмонин А.В. Методология криминалистической методики: монография. М.: Юрлитинформ, 2010. 416 с.
23. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. N 1.
24. Чеботарева А.А. Средства массовой информации в сети Интернет: проблемы юридической ответственности. Монография. Чита: ЧитГУ, 2009.
25. 9. Эйсман А.А. Теоретические вопросы программирования расследования // Вопросы борьбы с преступностью. Вып. 45. М., 1987. С. 84 - 85.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для изучения дисциплины

1. Электронная научная библиотека ДГУ. http://www.elib.dgu.ru
2. Электронная библиотека РГБ. http://www.lib 05. Ru
3. http://www.IQlib.ru - электронная библиотечная система «IQlib»

9.Методические указания для обучающихся по освоению дисциплины

В учебном процессе в рамках дисциплины выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях (как правило, в подгруппах) под непосредственным руководством преподавателя и по его заданиям. Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя,

но без его непосредственного участия. Внеаудиторная самостоятельная работа, как правило, связана с подготовкой к практическому занятию.

В рамках изучения дисциплины ' используются следующие виды заданий для самостоятельной работы:

- самостоятельное изучение темы теоретического курса;
- выполнение домашних заданий;
- подготовка к практическим занятиям и проблемным дискуссиям;
- подготовка докладов;
- подготовка к тестовым заданиям по усвоению материала.

По всем темам семинарских занятий студентам предлагается домашнее задание для подготовки к работе по заданиям преподавателя во время занятия.

При подготовке к занятиям и проблемным дискуссиям студентам необходимо пользоваться указанными преподавателем нормативно-правовыми актами, учебной и научной литературой, периодическими изданиями, а также практической информацией (статистическими данными, аналитическими данными, международными рейтингами и т.п.).

Структура курса выстроена таким образом, что каждая следующая тема базируется на знаниях предыдущей пройденной темы. Именно поэтому следует при самоподготовке уделять внимание повторению пройденных материалов.

В ряде тем предусмотрена подготовка студентами доклада и выступление с ним на занятии. Информация доклада, как правило, является базой для выполнения заданий в рамках занятия, поэтому студентам, готовящим доклад, следует убедиться, что в докладе отражены все вопросы, поставленные преподавателем.

Эссе - это форма задания, которая представляет собой один или несколько вопросов (заданий), на которые нужно ответить в свободной форме. Эссе оценивается по правилам или критериям, предназначенным для выявления умений творчески использовать полученные знания. Самостоятельная работа студентов состоит в творческом ответе на вопрос по выбранной теме эссе. Для этого студенту необходимо:

1.Из соответствующих печатных или электронных источников информации взять материалы, в которых рассматривается данная тема.

2.Проанализировать материалы, сравнить различные точки зрения по данному вопросу.

3.Тезисно изложить теорию, факты и взгляды специалистов, которые необходимо знать для понимания данного вопроса.

4.Сформировать и отразить в основной части письменной работы свою

авторскую позицию по вопросу.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- Технические средства: персональные компьютеры, проектор, интерактивная доска.
- Методы обучения с использованием информационных технологий: компьютерное тестирование, демонстрация мультимедийных материалов.
- Перечень Интернет- сервисов и электронных ресурсов: поисковые системы, электронная почта, профессиональные чаты, форумы, системы видеоконференций, электронные учебные и учебно-методические материалы.
- Перечень программного обеспечения: операционная система Microsoft Windows, MS Power Point для подготовки слайдов и призентаций.
- Перечень справочно-информационных систем ЭБС «Книгафонд», «Гарант», «Консультант Плюс», а также информацию, находящуюся в глобальной сети Internet.

11. Образовательные технологии

В соответствии с требованиями ФГОС ВПО по направлению подготовки 030900.62 Юриспруденция реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий. (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В качестве интерактивных форм обучения в процессе преподавания курса используется обмен данными различных форматов. В процессе изучения дисциплины используется информационная инфраструктура, которая включает различные технологии (оборудование, программное обеспечение, периферийные устройства и связь с Интернетом).

Удельный вес занятий, проводимых в интерактивных форма в семестрах составляет 30% аудиторных занятий (определяется в соответствии с требованиями ФГОС).

Для освоения бакалаврами учебной дисциплины, получения знаний и формирования общих компетенций используются следующие образовательные технологии:

-дискуссия;
-презентация;
-подготовка обзора научной литературы по теме;
-семинар-диспут
-решение задач;
-анализ конкретных ситуаций;

-«мини-конференция»;
-«круглый стол»;

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

Для проведения занятий имеются подготовленные аудитории к проведению занятий по настоящей учебной дисциплине, имеются стандартно оборудованные лекционные аудитории (доска, фломастеры для доски), мультимедийное оборудование и компьютерные классы с выходом в Интернет, специализированные оборудованные аудитории.