МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ПРАВА ЭКОНОМИКИ И ФИНАНСОВ

КАФЕДРА УГОЛОВНОГО ПРАВА, ПРОЦЕССА И КРИМИНАЛИСТИКИ

СОГЛАСОВАНО

Руководитель образовательной программы Р.С.Джинджолия

_____

«30» 05 2023 г.

УТВЕРЖДАЮ

Директор института Е.М. Машукова

_____

«30» 05 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки
40.04.01 ЮРИСПРУДЕНЦИЯ
(код и наименование направления подготовки)

Направленность (программа)
Уголовное право; криминология

Квалификация (степень) выпускника
Магистр

Форма обучения
(очная, заочная)

Нальчик 2023

Рабочая программа дисциплины (модуля) «Преступления в сфере информационной безопасности» / сост. ст. преподаватель Марзей А.А.. – Нальчик: КБГУ, 2023. – с. 33

Рабочая программа дисциплины (модуля) предназначена для обучающихся *очной* формы обучения по направлению подготовки 40.04.01 Юриспруденция, направленность (программа) «Уголовное право; криминология», 3 семестра, 2 года (ОФО).

Рабочая программа составлена с учетом федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 40.04.01 Юриспруденция, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 25.11.2020 г. № 1451 (Зарегистрировано в Минюсте России 09.03.2021 г. № 62681).

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины (модуля)

Дисциплина «Преступления в сфере информационной безопасности» имеет своей целью формирование у студентов 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 федеральным государственным образовательным стандартом высшего образования по направлению 40.04.01 «Юриспруденция».

Основными задачами изучения дисциплины «Преступления против информационной безопасности» 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.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «Преступления против информационной безопасности» относится к дисциплинам по выбору Блока 1. Дисциплины (модули) основной образовательной программы по направлению подготовки 40.04.01 Юриспруденция, дисциплины по выбору, направленность (программа): «Уголовное право; криминология».

Дисциплина позволит расширить теоретическую подготовку обучающегося, получить практические навыки информационной безопасности.

Освоение дисциплины «Преступления против информационной безопасности» необходимо для выполнения научно-исследовательской работы, подготовки к процедуре защиты и защиты выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины (модуля)

Дисциплина направлена на формирование следующей компетенции в соответствии с ФГОС ВО и ОПОП ВО – магистратуры по направлению подготовки 40.04.01 Юриспруденция:

Компетенция	Индикаторы компетенций	Результаты обучения
ПКС-2 Способен выявлять и применять нормы материального права в профессиональной деятельности	*ПКС-2.1 Способен осуществлять поиск и выявлять правовые нормы подлежащие применению*	**Знать:** основы и особенности логического мышления, анализа, систематизации, обобщения, критического осмысления информации, постановки исследовательских задач и выбора путей их решения.

		Уметь: логически мыслить, осуществлять постановку исследовательских задач и проводить анализ, систематизацию, обобщение, критическое осмысление используемой информации, выбирать пути решения поставленных задач **Владеть:** навыками логического мышления, анализа, систематизации, обобщения, критического осмысления информации, постановки исследовательских задач и выбора путей их решения в своей профессиональной деятельности
	ПКС-2.2 Способен применять необходимую правовую норму	**Знать:** основные виды, способы и особенности толкования нормативных правовых актов; содержание и основные правила юридической квалификации юридических фактов и связанных с ними обстоятельств при анализе преступлений против основ национальной безопасности. **Уметь:** определять виды и способы толкования нормативных правовых актов; выявлять факты и обстоятельства, требующие правовой квалификации, правильно определять круг нормативноправовых актов, нормы которых распространяются на данные факты и обстоятельства, давать юридическую оценку преступлениям против основ национальной безопасности. **Владеть:** навыками толкования нормативных правовых актов в своей профессиональной деятельности; навыками грамотного юридического анализа фактов,

		событий и обстоятельств и юридически правильной квалификации преступлений против основ информационной безопасности.

4. Содержание и структура дисциплины (модуля)

Таблица 1. Содержание дисциплины (модуля), перечень оценочных средств и контролируемых компетенций

№ п/п	Наименование раздела/ темы	Содержание раздела	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	2	3	4	5
1.	Информацион ная 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	ПКС-2.1, ПКС-2.2	(П), (К);
2.	Понятие и система преступлений против информационной безопасности по российскому уголовному законодательству.	1. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. Понятие киберпреступности. 2. Система преступлений против информационной безопасности по российскому уголовному законодательству. 3. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.	ПКС-2.1, ПКС-2.2	(П), (К);
3.	Уголовно-правовая характеристик а преступлений	1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).	ПКС-2.1, ПКС-2.2	(П), (К);

	против информационной безопасности по УК РФ	3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК). 4. Иные преступления против информационной безопасности по УК РФ. 5. Преступления против информационной безопасности, совершаемые с использованием глобальных компьютерных сетей.		
4.	Квалификация преступлений против информационной безопасности	1. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне. 2. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту. 3. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка. Типовые квалифицирующие признаки. 4. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет). 5. Проблемы квалификации иных преступлений против информационной безопасности.	ПКС-2.1, ПКС-2.2	(П), (К);
5.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты информационной безопасности	1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах. 2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации. 3. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран. 4. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.). 5. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).	ПКС-2.1, ПКС-2.2	(П), (К);

6.	Криминологические основы противодействия преступлениям против информационной безопасности	1.Современная криминологическая оценка преступности в сфере информационной безопасности. 2. Причины и условия преступлений против информационной безопасности. 3. Криминологические особенности личности преступника в сфере информационной безопасности и механизм преступного поведения. 4. Основные направления и меры предупреждения преступлений против информационной безопасности	ПКС-2.1, ПКС-2.2	(П), (К);

Структура дисциплины (модуля)

Таблица 2. Общая трудоемкость дисциплины (модуля) составляет 4 зачетные единицы (144 часа)

Вид работы	Трудоёмкость, часы	
	ОФО 1 курс	ЗФО Сессия №2
Общая трудоемкость (в часах)	**144**	**144**
Контактная работа (в часах):	***51***	***6***
Лекционные занятия (Л)	17	2
Практические занятия (ПЗ)	34	4
Семинарские занятия (СЗ)	Не предусмотрены	Не предусмотрена
Лабораторные работы (ЛР)	Не предусмотрены	Не предусмотрена
Самостоятельная работа (в часах), в том числе контактная (внеаудиторная) работа:	***84***	***134***
Расчетно-графическое задание (РГЗ)	Не предусмотрено	Не предусмотрено
Реферат (Р)	Не предусмотрены	Не предусмотрены
Эссе (Э)	Не предусмотрены	Не предусмотрены
Контрольная работа (КР)	Не предусмотрена	Не предусмотрена
Самостоятельное изучение разделов/тем	84	134
Курсовая работа (КР)/ Курсовой проект (КП)	Не предусмотрена	Не предусмотрена

Подготовка и прохождение промежуточной аттестации	**9**	**4**
Вид промежуточной аттестации	**Зачет**	**Зачет**

Таблица 3. Лекционные занятия

№ п/п	Тема
1.	1.Информационные отношения как предмет правового регулирования. 2.Понятие информационной безопасности. Источники угроз информационной безопасности. 3.Структура информационной безопасности как объекта уголовно - правовой охраны.
2.	1. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. Понятие киберпреступности. 2. Система преступлений против информационной безопасности по российскому уголовному законодательству.
3.	1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК). 3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).
4.	1. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне. 2. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту. 3. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка. Типовые квалифицирующие признаки.
5.	1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах. 2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации. 3. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.
6.	1.Современная криминологическая оценка преступности в сфере информационной безопасности. 2. Причины и условия преступлений против информационной безопасности.

Таблица 4. Практические занятия

№ п/п	Тема
1.	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. Ответ на семинаре, коллоквиум, собеседование, реферат 5. Законодательство РФ в области обеспечения информационной безопасности
2.	1. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. Понятие киберпреступности. 2. Система преступлений против информационной безопасности по российскому уголовному законодательству. 3. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.
3.	1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК). 3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК). 4. Иные преступления против информационной безопасности по УК РФ. 5. Преступления против информационной безопасности, совершаемые с использованием глобальных компьютерных сетей.
4.	1. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне. 2. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту. 3. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка. Типовые квалифицирующие признаки. 4. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет). 5. Проблемы квалификации иных преступлений против информационной безопасности
5.	1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах. 2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации. 3. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран. 4. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.). 5. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).
6.	1.Современная криминологическая оценка преступности в сфере информационной безопасности. 2. Причины и условия преступлений против информационной безопасности. 3. Криминологические особенности личности преступника в сфере информационной безопасности и механизм преступного поведения. 4. Основные направления и меры предупреждения преступлений против информационной безопасности.

Таблица 5. Лабораторные работы – не предусмотрены.

Таблица 6. Самостоятельное изучение разделов дисциплины

№ п/п	Вопросы, выносимые на самостоятельное изучение
1.	1. Информация как объект информационных отношений предмет преступлений против информационной безопасности. Категории информации по критериям доступа к ней и распространения. 2. Законодательство РФ в области обеспечения информационной безопасности
2.	1. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.
3.	1. Иные преступления против информационной безопасности по УК РФ. 2. Преступления против информационной безопасности, совершаемые с использованием глобальных компьютерных сетей.
4.	1. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет). 2. Проблемы квалификации иных преступлений против информационной безопасности.
5.	1. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.). 2. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).
6.	1. Криминологические особенности личности преступника в сфере информационной безопасности и механизм преступного поведения. 2. Основные направления и меры предупреждения преступлений против информационной безопасности

5.Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

В ходе изучения дисциплины предусматриваются ***текущий, рубежный контроль и промежуточная аттестация.***

5.1 Оценочные материалы для текущего контроля. *Цель текущего контроля* – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины *«Преступления против информационной безопасности»* и включает: ответы на теоретические вопросы на практическом занятии, решение практических задач и выполнение заданий на практическом занятии.

Оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы начисляются в зависимости от сложности задания.

<u>5.1.1. Вопросы по темам дисциплины «Преступления против информационной безопасности»</u> (контролируемые компетенций ПКС-2.1, ПКС-2.2и ОПК-7, индикаторы достижения компетенции ПКС-2.1, ПКС-2.2).

Контрольные вопросы по теме «Информационная безопасность как объект уголовно-правовой охраны».

1. 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.

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.

Контрольные вопросы по теме «Уголовно-правовая характеристика преступлений против информационной безопасности по УК РФ»

1. Дайте характеристику эволюции уголовного законодательства, предусматривающего ответственность за компьютерные преступления в России.

2. Дайте уголовно - правовую характеристику неправомерного доступа к компьютерной информации (ст. 272 УК).

3. Дайте уголовно - правовую характеристику создания, использования и распространения вредоносных программ для ЭВМ (ст. 273 УК). 27

4. Дайте уголовно - правовую характеристику нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).

5. Дайте уголовно - правовую характеристику иных преступлений, против информационной безопасности.

6. Назовите преступления против информационной безопасности, совершаемые с использованием глобальных компьютерных сетей.

Контрольные вопросы по теме «Квалификация преступлений против информационной безопасности»

1. Каковы основные проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.

2. Каковы основные проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.

3. Назовите квалифицированные виды преступлений в сфере компьютерной информации и дайте им уголовно – правовую оценку. Назовите типовые квалифицирующие признаки.

4. Каковы проблемы квалификации преступлений против информационной безопасности, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).

5. Каковы основные проблемы квалификации иных преступлений против информационной безопасности.

Контрольные вопросы по теме «Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты информационной безопасности»

1. Дайте характеристику основных подходы различных государств к криминализации преступлений в сфере информационной безопасности.

2. Проведите сравнительно-правовой анализ преступлений в сфере информационной безопасности в зарубежном уголовном законодательстве (на примере УК некоторых государств).

3. Назовите действующие международные соглашения в сфере борьбы с преступлениями против информационной безопасности.

4. Дайте характеристику Международной Конвенции по борьбе с киберпреступностью от 23 ноября 2001 г.

5. Назовите особенности правового регулирования борьбы с преступлениями против информационной безопасности в странах дальнего зарубежья и странах СНГ.

6. Дайте сравнительный анализ уголовной ответственности за отдельные преступления против информационной безопасности по законодательству стран ближнего зарубежья (по выбору).

7. Дайте сравнительный анализ уголовной ответственности за отдельные преступления против информационной безопасности по законодательству стран дальнего зарубежья (по выбору).

Контрольные вопросы по теме «Криминологические основы противодействия преступлениям против информационной безопасности»

1. Дайте оценку общественной опасности преступлений в сфере информационной безопасности.

2. Дайте характеристику основных криминологических показателей преступлений против информационной безопасности.

3. Дайте характеристику общественной опасности преступлений против информационной безопасности в глобальных компьютерных сетях.

4. Дайте характеристику латентности преступлений против информационной безопасности и методов ее определения.

5. Дайте криминологическую характеристику основных направлений профилактики преступлений против информационной безопасности.

6. Выявите основные проблемы правового регулирования борьбы с преступлениями против информационной безопасности на современном этапе.

7. Каковы особенности предупреждения преступлений против информационной безопасности в глобальных компьютерных сетях.

Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине *«Преступления против информационной безопасности»*. Развёрнутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

3 балла, ставится, если обучающийся:

1) полно излагает изученный материал, даёт правильное определенное понятий;
2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные;
3) излагает материал последовательно и правильно с точки зрения норм литературного языка.

2 балла, ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого.

1 балл, ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но:

1) излагает материал неполно и допускает неточности в определении понятий;
2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;
3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.

0 баллов, ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.

Баллы «3», «2», «1» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных обучающемся на протяжении занятия.

5.1.2. Оценочные материалы для самостоятельной работы обучающегося (типовые задачи) (контролируемые компетенций ПКС-2, индикаторы достижения компетенции ПКС-2.1, ПКС-2.2).

Перечень типовых задач для самостоятельной работы сформирован в соответствии с тематикой практических занятий по дисциплине «*Преступления против информационной безопасности*».

Методические рекомендации по решению задач

Обучающемуся, необходимо изучить предложенную преподавателем литературу и характеристику условий задачи, выбрать оптимальный вариант (подобрать известные и стандартные алгоритмы действия) или варианты разрешения контрольных заданий. Решение каждого контрольного задания должно заканчиваться выводом, в котором дается оценка полученных результатов.

Задача № 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.

Задача № 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.

Задача № 3

Ш. совместно с К. незаконно получили абонентские номера и шифркоды 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 32 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.

Задача № 4

П. вступил в сговор с сотрудником компании сотовой связи Д. При этом согласно имевшейся договоренности Д. снабжал П. информацией об электронном серийном номере (ESN), являющемся уникальным в общей массе электронных устройств стандарта связи CDMA и устанавливаемом на заводе-изготовителе телефонного аппарата, и о мобильном избирательном (абонентском) номере абонента (MIN), присваиваемом компаниейоператором сотовой связи. Сведения об ESN и MIN хранятся также в памяти центрального контроллера. При выходе абонента на связь центральный контроллер проверяет соответствие комбинации двух указанных номеров, записанных в памяти телефонного аппарата, с совокупностью комбинаций, хранящихся в его памяти. В случае, если обе комбинации совпадают, то центральный контроллер «пропускает» входящий или

исходящий звонок. П. осуществлял перепрограммирование телефонных аппаратов, вводя в их память значение ESN и MIN, полученные от Д., таким образом появлялись телефонные трубки-двойники. Их настройку, тестирование и введение в работу в качестве средств мобильной связи также осуществлял П. В результате действий П. и Д. произошло внесение несанкционированных изменений в техническую и биллинговую информацию, содержащуюся в центральном контроллере указанной сети, а также нарушение работы компьютерной сети компании.

Задача № 5

Р., зарегистрированная в качестве индивидуального предпринимателя, используя устройство для подключения к COM-порту, подключала его к 33 соответствующему разъему контрольно-кассовой машины АМС-100Ф, являющейся специализированной электронно-вычислительной машиной, в результате чего производила уменьшение фактической выручки, информация о которой содержалась в фискальной памяти кассового аппарата.

Задача № 6

М. приобрел за 1 тыс. дол. сотовый телефонный аппарат-двойник. В последующем М. предложил студентам Нижегородской академии гражданину Пакистана Э. и гражданину Бангладеш К. совместно использовать этот телефонный аппарат в корыстных целях, предоставляя возможность иностранным студентам осуществлять телефонные международные переговоры с этого аппарата по заниженным тарифам. Полученную прибыль они распределяли между собой. Во исполнение достигнутой договоренности Э. передал М. в качестве оплаты за приобретенный в совместную собственность сотовый телефонный аппарат 750 дол. М., Э. и К. производили телефонные междугородние звонки своим родственникам, знакомым, без оплаты их стоимости оператору сотовой связи. В этот же период М., Э. и К. для проживающих в общежитии иностранных студентов организовали возможность использовать указанный телефонный аппарат для звонков в различные страны мира и получали со студентов за эти переговоры по 8 р. за каждую минуту. В общей сложности ими было произведено 549 таких соединений на сумму 26 720 р. 80 к., за которые они получили 500 дол. и поделили их между собой согласно достигнутой ранее договоренности.

Критерии формирования оценок по заданиям для самостоятельной работы обучающегося (типовые задания):

«отлично» (3 балла) - обучающийся показал глубокие знания материала по поставленным вопросам, грамотно, логично его излагает, структурировал и детализировал информацию, избегая простого повторения информации из текста, информация представлена в переработанном виде. Свободно использует необходимые формулы при решении задач;

«хорошо» (2 балла) - обучающийся твердо знает материал, грамотно его излагает, не допускает существенных неточностей в процессе решения задач;

«удовлетворительно» (1 балл) - обучающийся имеет знания основного материала по поставленным вопросам, но не усвоил его деталей, допускает отдельные неточности при решении задач;

«неудовлетворительно» (0 баллов) – обучающийся, допускает грубые ошибки в ответе на поставленные вопросы и при решении задач.

5.2. Оценочные материалы для рубежного контроля (контролируемые компетенций ПКС-2, индикаторы достижения компетенции ПКС-2.1, ПКС-2.2).

Рубежный контроль осуществляется по более или менее самостоятельным разделам – учебным модулям курса и проводится по окончании изучения материала модуля в

заранее установленное время. Рубежный контроль проводится с целью определения качества усвоения материала учебного модуля в целом. В течение семестра проводится ***три таких контрольных мероприятия по графику***.

В качестве форм рубежного контроля можно использовать проведение коллоквиума или контрольных работ. На рубежные контрольные мероприятия рекомендуется выносить весь программный материал (все разделы) по дисциплине.

5.2.1. Промежуточное контрольно-рейтинговое мероприятие №1. 23 балла (тест, коллоквиум)

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.

7. Система преступлений против информационной безопасности по российскому уголовному законодательству.

8. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.

Промежуточное контрольно-рейтинговое мероприятие №2. 23 балла (тест, коллоквиум)

9.Неправомерный доступ к компьютерной информации (ст. 272 УК).

10. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).

11. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).

12. Иные преступления против информационной безопасности по УК РФ.

13. Преступления против информационной безопасности, совершаемые с использованием глобальных компьютерных сетей.

14. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.

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

Промежуточное контрольно-рейтинговое мероприятие №3. 24 балла (тест, коллоквиум)

16. Проблемы квалификации иных преступлений против информационной безопасности.

17. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах.

18. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.

19. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.

20. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.).

21. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).

Критерии формирования оценок по контрольным точкам (коллоквиум)

Коллоквиум является одним из основных способов учета знаний обучающихся по дисциплине. Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения. При оценке ответа обучающегося необходимо руководствоваться следующими критериями:

– полнота и правильность ответа;
– степень осознанности, понимания изученного;
– языковое оформление ответа.

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.

1) «отлично» (5-6 баллов) - правильные ответы даны на 75-100% вопросов;
2) «хорошо» (3-4 балла) - правильные ответы даны на 51-75% вопросов;
3) «удовлетворительно» (1-2 балла) - если правильные ответы даны на 26-50% вопросов;
4) «неудовлетворительно» (0 баллов) - правильные ответы даны менее чем на 25% включительно.

5.3 Оценочные материалы для промежуточной аттестации.

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися. Промежуточная аттестация предназначена для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины. Осуществляется в конце семестра и представляет собой итоговую оценку знаний по дисциплине «*Преступления против информационной безопасности*» в виде проведения зачета.

Промежуточная аттестация может проводиться в устной или письменной форме. На промежуточную аттестацию отводится до 30 баллов.

Перечень вопросов для промежуточной аттестации (зачет)
(контролируемые компетенций ПКС-2.1, индикаторы достижения компетенции ПКС-2.1, ПКС-2.2).

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.. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений.

6. Система преступлений против информационной безопасности по российскому уголовному законодательству.
7. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.
8. Особенности объекта и предмета преступлений против информационной безопасности
9. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
10. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).
11. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).
12. Проблемы квалификации преступлений против информационной безопасности (общая характеристика).
13. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.
14. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.
15. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка. Типовые квалифицирующие признаки.
16. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).
17. Проблемы квалификации иных преступлений против информационной безопасности.
18. Отграничение преступлений против информационной безопасности от смежных составов преступлений.
19. Общая характеристика международного законодательства в сфере борьбы с киберпреступностью.
20. Понятие киберпреступности в международном уголовном праве.
21. Основные направления международного сотрудничества в борьбе с киберпреступностью.
22. Ответственность за преступления против информационной безопасности в странах СНГ.
23. Органы, осуществляющие борьбу с преступлениями против информационной безопасности .
24. Особенности борьбы преступлениями против информационной безопасности в глобальных компьютерных сетях.
25. Состояние, уровень, структура, динамика преступлений против информационной безопасности.
26. Причины и условия преступлений против информационной безопасности в современных условиях.
27. Характеристика личности преступника в сфере информационной безопасности.
28. Законодательство РФ в области обеспечения информационной безопасности
29. Основы предупреждения преступлений против информационной безопасности .
30. Правовое регулирование борьбы с преступлениями против информационной безопасности .
31. Принципы борьбы с преступлениями против информационной безопасности.
32. Основные направления предупреждения преступлений против информационной безопасности.

Критерии формирования оценок по промежуточной аттестации:

Оценка выполнения практического задания	до 15 баллов
Оценка собеседования по теоретической части	до 10 баллов
Критерии оценки (результат определяется как сумма всех составляющих)	

«Зачтено» (61 и более баллов)	Выполнение практической части: – задание выполнено в объеме более 60% с соблюдением необходимой последовательности действий; – без существенных ошибок выполнены все записи, таблицы, рисунки, вычисления, допускаются погрешности в оформлении работы; – проявлен достаточный уровень умений применять знания и методы для решения практических задач/заданий; – проявлено владение навыками использования полученных теоретических знаний и практических умений в сфере профессиональной деятельности. Собеседование по теоретической части: – демонстрирует знание основных категорий, допускаются неточности в их объяснении; – демонстрирует понимание приобретенных знаний и умений для будущей профессиональной деятельности.
«Не зачтено» (менее 61 балла)	Выполнение практической части: – задание выполнено в объеме менее 60%, нарушена последовательность действий, что привело к существенным ошибкам и неверным выводам; – с существенными или грубыми ошибками выполнены записи, таблицы, рисунки, вычисления; – проявлен неудовлетворительный уровень умений применять знания и методы для решения практических задач/заданий; – не может показать навыки использования полученных знаний в будущей профессиональной деятельности. Собеседование по теоретической части: – не имеет представления о категориях, испытывает сложности при выборе методов объяснения их; – демонстрирует непонимание приобретенных знаний и умений для будущей профессиональной деятельности.

Виды ошибок

1. Грубые ошибки:

- незнание определений основных понятий, законов, правил, основных положений теории;
- неумение выделить в ответе главное;
- незнание приемов решения заданий, ошибки, показывающие неправильное понимание условия контрольной работы или неправильное истолкование решения.

2. Негрубые ошибки:

- неточности формулировок, определений, понятий, законов, теорий, вызванные неполнотой охвата основных признаков определяемого понятия;
- нерациональный выбор хода решения.

3. Недочеты:

- нерациональные приемы решения заданий;

- отдельные погрешности в формулировке ответа;
- небрежное выполнение задания.

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

Для допуска к зачету студент должен набрать в ходе текущего и рубежного контроля успеваемости не менее 36 баллов.

Для получения зачета, которым заканчивается изучение дисциплины в семестре, студенту необходимо иметь не менее 61 балла. Если по итогам текущего и рубежного контроля успеваемости студент набрал число баллов в пределах 36 < (Sтек.+Sруб) <61, то он допускается к сдаче зачета. По итогам сдачи зачета он может повысить сумму баллов до 61 (не более), необходимых для получения зачета.

Общий балл текущего и рубежного контроля складывается из следующих составляющих **Приложение 2.**

Целью промежуточной аттестации по дисциплине является оценка качества освоения дисциплины обучающимися.

Критерии оценки качества освоения дисциплины **(Приложение 3).**

Типовые задания, обеспечивающие формирование компетенций ПКС-2., а также индикаторы достижения компетенций ПКС-2.1, ПКС-2.2 представлены в таблице 7

Таблица 7. Результаты освоения учебной дисциплины, подлежащие проверки

Код и наименование общепрофессиональной компетенции выпускника: *ПКС-2 Способен выявлять и применять нормы материального права в профессиональной деятельности* **Код и наименование индикатора достижения общепрофессиональной компетенций выпускника:** *ПКС-2.1 Способен осуществлять поиск и выявлять правовые нормы подлежащие применению*	**Знать:** основные виды, способы и особенности толкования нормативных правовых актов; содержание и основные правила юридической квалификации юридических фактов и связанных с ними обстоятельств при анализе преступлений против основ национальной безопасности.	Оценочные материалы для текущего контроля (раздел 5.1.1). Оценочные материалы для самостоятельной работы (раздел 5.1.2). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для промежуточной аттестации (раздел 5.3).
	Уметь: определять виды и способы толкования нормативных правовых актов; выявлять факты и обстоятельства, требующие правовой квалификации, правильно определять круг нормативноправовых актов, нормы которых распространяются на данные факты и обстоятельства, давать юридическую оценку преступлениям против	Оценочные материалы для текущего контроля (раздел 5.1.1). Оценочные материалы для самостоятельной работы (раздел 5.1.2). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для промежуточной аттестации (раздел 5.3).

	основ национальной безопасности.	
	Владеть: навыками толкования нормативных правовых актов в своей профессиональной деятельности; навыками грамотного юридического анализа фактов, событий и обстоятельств и юридически правильной квалификации преступлений против основ информационной безопасности.	Оценочные материалы для текущего контроля (раздел 5.1.1). Оценочные материалы для самостоятельной работы (раздел 5.1.2). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для промежуточной аттестации (раздел 5.3).
Код и наименование общепрофессиональной компетенции выпускника: *ПКС-2 Способен выявлять и применять нормы материального права в профессиональной деятельности*	**Знать:** основы и особенности логического мышления, анализа, систематизации, обобщения, критического осмысления информации, постановки исследовательских задач и выбора путей их решения.	Оценочные материалы для текущего контроля (раздел 5.1.1). Оценочные материалы для самостоятельной работы (раздел 5.1.2). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для промежуточной аттестации (раздел 5.3).
Код и наименование индикатора достижения общепрофессиональной компетенций выпускника: *ПКС-2.2 Способен применять необходимую правовую норму*	**Уметь:** логически мыслить, осуществлять постановку исследовательских задач и проводить анализ, систематизацию, обобщение, критическое осмысление используемой информации, выбирать пути решения поставленных задач	Оценочные материалы для текущего контроля (раздел 5.1.1). Оценочные материалы для самостоятельной работы (раздел 5.1.2). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для промежуточной аттестации (раздел 5.3).
	Владеть: навыками логического мышления, анализа, систематизации, обобщения, критического осмысления информации, постановки исследовательских задач и выбора путей их решения в своей профессиональной	Оценочные материалы для текущего контроля (раздел 5.1.1). Оценочные материалы для самостоятельной работы (раздел 5.1.2). Оценочные материалы для коллоквиума (раздел 5.2.1). Оценочные материалы для

	деятельности	промежуточной аттестации (раздел 5.3).

7. Учебно-методическое обеспечение дисциплины (модуля)

7.1. Нормативно-законодательные акты

1. Конституция РФ 1993 г. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.
2. Уголовный кодекс РФ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.
3. Уголовно-процессуальный кодекс РФ. – [Электронный ресурс]. – Режим доступа: Консультант Плюс: URL: www. consultant.ru.
4.

7.2 Основная литература

1. Бобраков И.А. Уголовное право [Электронный ресурс] : учебник / И.А. Бобраков. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 736 c. — 978-5-4487-0189-4. — Режим доступа: http://www.iprbookshop.ru/73870.html
2. Уголовное право России. Общая часть [Электронный ресурс] : учебник / Л.В. Бакулина [и др.]. — Электрон. текстовые данные. — М. : Статут, 2016. — 864 c. — 978-5-8354-1274-7. — Режим доступа: http://www.iprbookshop.ru/58290.html
3. Уголовное право Российской Федерации. Общая часть [Электронный ресурс] : учебник / В.В. Бабурин [и др.]. — 3-е изд. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016. — 448 c. — 978-5-88651-621-0. — Режим доступа: http://www.iprbookshop.ru/72877.html

7.3 Дополнительная литература

1. Голованова Н.А. Уголовное право зарубежных стран. Общая и Особенная части [Электронный ресурс] : учебник / Н.А. Голованова, В.Н. Еремин, М.А. Игнатова. — Электрон. текстовые данные. — М. : Волтерс Клувер, 2010. — 1056 c. — 978-5-466-00507-3. — Режим доступа: http://www.iprbookshop.ru/16807.html

2. Уголовное право Российской Федерации. Общая часть [Электронный ресурс] : учебник для вузов / Н.Н. Белокобыльский [и др.]. — Электрон. текстовые данные. — М. : Статут, 2014. — 879 c. — 978-5-8354-0999-0. — Режим доступа: http://www.iprbookshop.ru/29091.html
3. Уголовное право России. Части общая и особенная. Учебник/Под ред. А.И. Рарога. М.: Проспект, 2014. 784 с.
4. Захарова Т.П. Уголовное право. Практикум [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по специальности «Юриспруденция»/ Захарова Т.П., Колоколов Н.А., Ярцев Р.В.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 479 c.— Режим доступа: http://www.iprbookshop.ru/52578.— ЭБС «IPRbooks»
5. Уголовное право Российской Федерации в схемах [Электронный ресурс]: учебное пособие / Бриллиантов А. В., Четвертакова Е. Ю. - М. : Проспект, 2018. - http://www.studentlibrary.ru/book/ISBN9785392271474.html

7.4. Периодические издания (газета, вестник, бюллетень, журнал)

1. Вестник МГУ серия 11 Право – библиотека КБГУ;
2. Высшее образование сегодня – библиотека КБГУ;
3. Высшее образование в России – библиотека КБГУ;
4. Известия вузов. Правоведение – библиотека КБГУ;
5. Известия вузов. Северо-Кавказский регион. Общественные науки – библиотека КБГУ;
6. История государства и права – библиотека КБГУ;
7. Российская юстиция – библиотека КБГУ;
8. Трудовое право – библиотека КБГУ;
9. Уголовное право – библиотека КБГУ.

7.5. Интернет-ресурсы

1. www.hro.org – Права человека в России.
2. www.supcourt.ru – Верховный суд Российской Федерации.
3. www.ksrf.ru – Конституционный Суд РФ
4. https://genproc.gov.ru – Генеральная прокуратура РФ
5. https://sledcom.ru – Следственный комитет РФ

– ***информационные справочные системы:***

1. Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru
2. Справочная правовая система «Гарант» (в свободном доступе). URL: http://www.garant.ru;
3. Справочная правовая система «Референт» (в свободном доступе). URL: https://www.referent.ru/
4. Информационно-справочная система «Аюдар Инфо» (в свободном доступе). URL: https://www.audar-info.ru/

– ***профессиональные базы данных:***

1. Национальная информационно-аналитическая система База данных Science Index (РИНЦ). URL: http://elibrary.ru
2. Национальная электронная библиотека РГБ (имеется режим для людей с нарушением зрения (для слепых и слабовидящих). URL: https://нэб.рф
3. ЭБД РГБ (библиотека диссертаций) (КК, ОДА, ИЗ, ИС*). URL: http://www.diss.rsl.ru
4. ЭБС «АйПиЭрбукс» (имеется режим для людей с нарушением зрения (для слабовидящих). URL: http://iprbookshop.ru/

7.6 Методические указания по проведению различных учебных занятий, к курсовому

проектированию и другим видам самостоятельной работы

При изучении курса рекомендуется следующая последовательность обучения: вначале обучающемся необходимо ознакомиться с рабочей программой курса и методическими указаниями по его изучению; проработать учебный материал по учебникам и лекциям, затем следует обратиться к дополнительной юридической литературе и нормативным актам. Обязательным условием закрепления и углубления знаний является участие обучающегося в практических занятиях, подготовка контрольной работы, написание реферата, а также самостоятельное решение задач.

Методические рекомендации при работе над конспектом во время проведения лекции.

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий. В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д.

Методические рекомендации по подготовке к практическим занятиям.

Практические (семинарские) занятия – составная часть учебного процесса, групповая форма занятий при активном участии обучающихся. Практические занятия способствуют углубленному изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся. Целью практических занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к семинарскому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем практические задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы.

Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

На практических занятиях обучающиеся учатся грамотно излагать проблемы, свободно высказывать свои мысли и суждения, рассматривают ситуации, способствующие развитию профессиональной компетентности. Следует иметь в виду, что подготовка к практическому занятию зависит от формы, места проведения семинара, конкретных заданий и поручений.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа (по В.И. Далю «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения обучающимися новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

– оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;

– широкое внедрение компьютеризированного тестирования;

– совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;

– модернизацию системы курсового проектирования, которая должна повышать роль обучающегося в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит обучающегося к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

– развивающую;

– информационно-обучающую;

– ориентирующую и стимулирующую;

– воспитывающую;

– исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разноуровневых задач и заданий;
3. Работа с тестами и вопросами для самопроверки;

Обучающимся рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые обучающийся получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Самостоятельная работа обучающихся предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости обучающийся может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее обучающимся и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать задачи и получать знания. Использование сетей усиливает роль самостоятельной работы обучающегося и позволяет кардинальным образом изменить методику преподавания.

Обучающийся может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Обучающийся имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде обучающегося имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет обучающемуся своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность обучающемуся сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов обучающийся будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.

2. Прием постановки вопросов к тексту имеет следующий алгоритм:

- медленно прочитать текст, стараясь понять смысл изложенного;
- выделить ключевые слова в тексте;

– постараться понять основные идеи, подтекст и общий замысел автора.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к зачету должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

Методические рекомендации для подготовки к зачету

Зачет является формой итогового контроля знаний и умений обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой. К зачету допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На зачете студент может набрать до 25 баллов.

В период подготовки к зачету обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к зачету включает три этапа:

– самостоятельная работа в течение семестра;
– непосредственная подготовка в дни, предшествующие зачету по темам курса;
– подготовка к ответу на зачетные вопросы.

При подготовке к зачету обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

8.Материально-техническое обеспечение дисциплины

Требования к материально-техническому обеспечению

Для реализации рабочей программы дисциплины имеются специальные помещения для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы (ауд. № 145 ГУК) и помещения для хранения и профилактического обслуживания оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средства обучения, служащими для представления информации большой аудитории.

При проведении занятий лекционного типа/семинарского типа используются:

лицензионное программное обеспечение:

– Лицензия на офисное программное обеспечение Мой Офис Стандартный;
– Лицензия на программное обеспечение средств антивирусной защиты Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1000-1500 Node 1 year Educational Renewal License (KL4863RAVFQ);
– Права на программное обеспечение для работы с PDF-документами ABBYY FineReader 15 Business;

свободно распространяемые программы:

– 7Z – программа-архиватор;
– Adobe Acrobat Reader – программа для чтения PDF файлов;
– Mozilla Firefox, Yandex – интернет-браузеры.

При осуществлении образовательного процесса обучающимися и преподавателем используются следующие информационные справочные системы: ЭБС «АйПиЭрбукс», СПС «Консультант плюс», СПС «Гарант», СПС «Референт», СПС «Аюдар Инфо».

Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;

2. Для инвалидов с нарушениями зрения (слабовидящие, слепые)

- присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для обучающихся с нарушениями зрения;
- задания для выполнения на экзамене зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

- на зачете/экзамене присутствует ассистент, оказывающий обучающемуся необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- зачет/экзамен проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию обучающегося экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Материально-техническое обеспечение дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Аудитория для самостоятельной работы и коллективного пользования специальными техническими средствами для обучения инвалидов и лиц с ОВЗ в КБГУ, аудитория No 145	- Комплект учебной мебели: столы и стулья для обучающихся (3 комплекта); Стол для инвалидов-колясочников (1 шт.); Компьютер с подключением к сети и программным	Продукты MICROCOFT(Desktop Education ALNG LicSaPk OLVS Academic Edition Enterprise) подписка (Open Value Subscription) No V 2123829 Kaspersky Endpoint Security

Главный корпус КБГУ.	обеспечением (3 шт.); Специальная клавиатура (с увеличенным размером клавиш, со специальной накладкой, ограничивающей случайное нажатие соседних клавиш) (1шт.); Принтер для печати рельефно-точечным шрифтом Брайля VP Columbia (1 шт.); Портативный тактильный дисплей Брайля «Focus 14 Blue» (совместимый с планшетными устройствами, смартфонами и ПК) (1 шт.); Бумага для печати рельефно-точечным шрифтом Брайля, совместимого с принтером VP Columbia; Видеоувеличитель портативный HV-MVC, диагональ экрана – 3,5 дюйма (4 шт.); Сканирующая и читающая машина SARA-CE (1 шт.); Джойстик компьютерный адаптированный, беспроводной (3 шт.); Беспроводная Bluetooth гарнитура с костной проводимостью «AfterShokz Trekz Titanium» (1 шт.); Проводная гарнитура с костной проводимостью «AfterShokz Sportz Titanium» (2 шт.); Проводная гарнитура Defender (1 шт.); Персональный коммуникатор EN –101 (5 шт.); Специальные клавиатуры (с увеличенным размером клавиш, со специальной накладкой, ограничивающей случайное нажатие соседних клавиш); Клавиатура адаптированная с крупными кнопками + пластиковая накладка, разделяющая клавиши, Беспроводная Clevy Keyboard + Clevy Cove (3шт.); Джойстик компьютерный Joystick SimplyWorks беспроводной (3шт.); Ноутбук + приставка для айтрекинга к ноутбуку PCEye Mini (1 шт).	Стандартный Russian Edition No Лицензии 17E0-180427-50836-287-197. Программы для создания и редактирования субтитров, конвертирующее речь в текстовый и жестовый форматы на экране компьютера: Майкрософт Диктейт: https://dictate.ms/, Subtitle Edit, («Сурдофон» (бесплатные). Программа невизуального доступа к информации на экране компьютера JAWS for Windows (бесплатная); Программа для чтения вслух текстовых файлов (Tiger Software Suit (TSS)) (номер лицензии 5028132082173733); Программа экранного доступа с синтезом речи для слепых и слабовидящих (NVDA) (бесплатная).

*Специальные помещения - учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы

Приложение 1

9. Лист изменений (дополнений) в рабочей программе дисциплины (модуля)

в рабочую программу по дисциплине «*Преступления против информационной безопасности*» по направлению подготовки 40.04.01 Юриспруденция, Направленность (программа) «Уголовное право; криминология» на 20_____- 20_____ учебный год

№ п/п	Элемент (пункт) РПД	Перечень вносимых изменений (дополнений)	Примечание

Обсуждена и рекомендована на заседании кафедры уголовного права, процесса и криминалистики протокол №_____от «_____» _____20_____г.

Заведующий кафедрой _____/Жиров Р.М.

10. Приложения

Приложение 2

Распределение баллов текущего и рубежного контроля

№п/п	*Вид контроля*	*Сумма баллов*			
		Обшая сумма	*1-я точка*	*2-я точка*	*3-я точка*
1-	***Посещение занятий***	***до 10 баллов***	***до 3 б.***	***до 3б.***	***до 4б.***
2-	***Текущий контроль:***	***до 42 баллов***	***до 14 б.***	***до 14 б.***	***до 14 б.***
	Полный правильный ответ	до 42 баллов	14 б.	14 б.	14 б.
	Неполный правильный ответ	от 3 до21 б.	от 1 до 7 б.	от 1 до 7 б.	от 1 до 7 б.
1.	***Рубежный контроль***	***до 18 баллов***	***до 6 б.***	***до 6 б.***	***до 6 б.***
	коллоквиум	от 0 до 18б.	от 0 до 6 б.	от 0 до 6 б.	от 0 до 6 б.
	Итого сумма текущего и рубежного контроля	***до 70 баллов***	***до 23 б.***	***до 23 б***	***до 24 б***

Приложение 3

Шкала оценивания планируемых результатов обучения

Текущий и рубежный контроль

Семестр	Шкала оценивания			
	0-35 баллов	36-50 баллов	51-60 баллов	56-70 баллов
	Частичное посещение аудиторных занятий. Неудовлетворительное выполнение лабораторных и практических работ. Плохая подготовка к балльно-рейтинговым мероприятиям. Обучающийся не допускается к промежуточной аттестации	Полное или частичное посещение аудиторных занятий. Частичное выполнение и защита лабораторных и практических работ. Ответы на коллоквиуме на оценку «удовлетворительно».	Полное или частичное посещение аудиторных занятий. Полное выполнение и защита лабораторных и практических работ. Ответы на коллоквиуме на оценку «хорошо».	Полное посещение аудиторных занятий. Полное выполнение и защита лабораторных и практических занятий. Ответы на коллоквиуме на оценку «отлично».

Зачет

Семестр	Шкала оценивания	
	Незачтено (36-60)	Зачтено (61-70)
	Студент имеет 36-60 баллов по итогам текущего и рубежного контроля, на зачёте не ответил ни на один вопрос.	Студент имеет 36-45 баллов по итогам текущего и рубежного контроля, на зачете представил полный ответ на один вопрос и частично (полностью) ответил на второй. Студент имеет 46-60 баллов по итогам текущего и рубежного контроля, на зачете дал полный ответ на один вопрос или частично ответил на оба вопроса. Студенту, имеющему 61-70 баллов по итогам текущего и рубежного контроля, выставляется отметка «зачтено» без сдачи зачёта.