

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Таганрогского института
имени А. П. Чехова (филиала)
РГЭУ (РИНХ)
_____ С. А. Петрушенко
«20» мая 2025 г.

**Рабочая программа дисциплины
Преступления в сфере компьютерной информации**

Направление подготовки
40.03.01 Юриспруденция

Направленность (профиль) программы бакалавриата
40.03.01.01 Уголовно-правовой

Для набора 2025 года

Квалификация
Бакалавр

КАФЕДРА отраслевых юридических дисциплин**Распределение часов дисциплины по семестрам / курсам**

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	13 1/6			
Неделя				
Вид занятий	уп	рп	уп	рп
Лекции	4	4	4	4
Практические	8	8	8	8
Итого ауд.	12	12	12	12
Контактная работа	12	12	12	12
Сам. работа	96	96	96	96
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.02.2025 протокол № 9.

Программу составил(и): канд. юрид. наук, Доц., Пашковский П.В.

Зав. кафедрой: канд. юрид. наук, доцент Курилкина О. А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	- формирование и развитие у будущих юристов теоретических знаний и практических навыков, связанных с организацией компьютерной безопасности, планированием, подготовкой и реализацией процесса обеспечения компьютерной безопасности;
1.2	- ознакомление студентов с методами и средствами защиты информации, организационными и правовыми мерами по информационной защите;
1.3	- ознакомление с совокупностью современных приемов поиска, исследования и фиксации информации при расследовании компьютерных преступлений.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен:

Знать:

основные методы, способы и средства получения, хранения, переработки информации (соотносится с индикатором ОПК-9.1, ПК-4.1);
закономерности обращения информации в правовой сфере (соотносится с индикатором ОПК-2.1, ОПК-8.1, ПК-7.3);
методы и способы защиты информации (соотносится с индикатором УК-1.1);
методы законного получения, хранения и переработки информации.

Уметь:

пользоваться основными методами, способами и средствами получения, хранения, переработки информации (соотносится с индикатором ОПК-9.2, ОПК-8.2);
соблюдать основные требования компьютерной безопасности, получать, хранить, перерабатывать использовать информацию (соотносится с индикатором ОПК-2.2, ПК-4.2, ПК-7.2);
правильно давать оценку информации (соотносится с индикатором УК-1.2).

Владеть:

навыками поиска, получения, хранения, переработки и защиты компьютерной информации, навыками сбора и обработки информации (соотносится с индикатором ОПК-9.3, ОПК-8.3);
навыками анализа информации (соотносится с индикатором ОПК-2.2, ПК-4.3, ПК-7.1);
навыками обработки информации (соотносится с индикатором УК-1.3).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы компьютерной безопасности

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Тема 1. Криминалистическая характеристика преступлений в сфере компьютерной информации Компьютерная информация. Понятие компьютерного преступления. Классификация компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Признаки и элементы состава преступления. Личностная характеристика преступника, совершающего компьютерное преступление. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.	Лекционные занятия	7	2	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
1.2	Тема 1. Криминалистическая характеристика преступлений в сфере компьютерной информации Компьютерная информация. Понятие компьютерного преступления.	Практические занятия	7	2	ОПК-9 УК-1 ОПК-2 ОПК-8

	<p>Классификация компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Признаки и элементы состава преступления.</p> <p>Личностная характеристика преступника, совершающего компьютерное преступление. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.</p>				<p>ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3</p>
1.3	<p>Тема 1. Криминалистическая характеристика преступлений в сфере компьютерной информации Компьютерная информация. Понятие компьютерного преступления.</p> <p>Классификация компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Признаки и элементы состава преступления.</p> <p>Личностная характеристика преступника, совершающего компьютерное преступление. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.</p>	Самостоятельная работа	7	14	<p>ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3</p>
1.4	<p>Тема 2. Правовое и организационное обеспечение компьютерной безопасности Понятие правового обеспечения компьютерной безопасности.</p> <p>Уголовное преследование за совершение компьютерных преступлений.</p> <p>Понятие каналов утечки информации. Организационно-административные мероприятия. Организационно-технические мероприятия.</p>	Лекционные занятия	7	2	<p>ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3</p>
1.5	<p>Тема 2. Правовое и организационное обеспечение компьютерной безопасности Понятие правового обеспечения компьютерной безопасности.</p> <p>Уголовное преследование за совершение компьютерных преступлений.</p> <p>Понятие каналов утечки информации. Организационно-административные мероприятия. Организационно-технические мероприятия.</p>	Практические занятия	7	2	<p>ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3</p>

					УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
1.6	<p>Тема 2. Правовое и организационное обеспечение компьютерной безопасности. Понятие правового обеспечения компьютерной безопасности.</p> <p>Уголовное преследование за совершение компьютерных преступлений.</p> <p>Понятие каналов утечки информации. Организационно-административные мероприятия. Организационно-технические мероприятия.</p>	Самостоятельная работа	7	14	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
1.7	<p>Тема 3. Способы совершения компьютерных преступлений. Компьютерные манипуляции. Компьютерный шпионаж и кража программ. Компьютерный саботаж. Компьютерные злоупотребления.</p> <p>Перехват информации. Несанкционированный доступ к информации.</p> <p>Способы нарушения конфиденциальности и целостности компьютерной информации.</p>	Практические занятия	7	2	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
1.8	<p>Тема 3. Способы совершения компьютерных преступлений. Компьютерные манипуляции. Компьютерный шпионаж и кража программ. Компьютерный саботаж. Компьютерные злоупотребления.</p> <p>Перехват информации. Несанкционированный доступ к информации.</p> <p>Способы нарушения конфиденциальности и целостности компьютерной информации.</p>	Самостоятельная работа	7	14	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2

					ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
1.9	Тема 4. Особенности образования следов по делам о компьютерных преступлениях Понятие и классификация следов компьютерных преступлений. Структурные файловые следы. Внешние файловые следы. Локальные файловые следы. Сетевые файловые следы. Следы – предметы. Следы-вещества. Регистрационные файлы операционных систем. Политика учетных записей. Политика прав пользователей. Политика аудита.	Практические занятия	7	2	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
1.10	Тема 4. Особенности образования следов по делам о компьютерных преступлениях Понятие и классификация следов компьютерных преступлений. Структурные файловые следы. Внешние файловые следы. Локальные файловые следы. Сетевые файловые следы. Следы – предметы. Следы-вещества. Регистрационные файлы операционных систем. Политика учетных записей. Политика прав пользователей. Политика аудита.	Самостоятельная работа	7	14	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
Раздел 2. Методика расследования компьютерных преступлений					
№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
2.1	Тема 5. Осмотр места происшествия по делам о компьютерных преступлениях Понятие осмотра места происшествия. Задачи следственного осмотра. Подготовительный этап осмотра места происшествия. Рабочий этап осмотра места происшествия. Криминалистическое исследование компьютерных систем и их сетей. Криминалистическое исследование операционных систем.	Самостоятельная работа	7	14	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1

					ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
2.2	<p>Тема 6. Изъятие следов компьютерных преступлений Понятие изъятия следов компьютерных преступлений. Фиксация следовой информации по делам о преступлениях. Резервное копирование файлов серверов. Документы со следами действий операционных систем. Документы со следами действий аппаратуры. Составление протокола изъятия следов.</p>	Самостоятельная работа	7	8	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
2.3	<p>Тема 7. Проведение компьютерно-технической экспертизы Понятие компьютерно-технической экспертизы. Аппаратно-компьютерная экспертиза. Программно-компьютерная экспертиза. Информационно-компьютерная экспертиза. Компьютерно-сетевая экспертиза. Комплексные экспертизы.</p>	Самостоятельная работа	7	8	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
2.4	<p>Тема 8. Ответственность за компьютерные преступления Уголовная ответственность за преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Ответственность за неправомерный доступ к компьютерной информации. Ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Международный опыт борьбы с преступлениями в сфере компьютерной информации.</p>	Самостоятельная работа	7	10	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3

					ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3
2.5	Подготовка к промежуточной аттестации	Зачет	7	0	ОПК-9 УК-1 ОПК-2 ОПК-8 ПК-4 ПК-7 ОПК-9.1 ОПК-9.2 ОПК-9.3 УК-1.1 УК-1.2 УК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-8.1 ОПК-8.2 ОПК-8.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Сверчков, Владимир Викторович	Уголовное право. Общая и Особенная части: учеб. пособие	М.: Юрайт, 2011	20 экз.
2	Пионтковский А. А.	Наука уголовного права	Санкт-Петербург: Лань, 2013	http://e.lanbook.com/books/element.php?p11_cid=25&p11_id=30479

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Зубарев, Сергей Михайлович, Казакова, В. А.	Уголовно-исполнительное право: учеб. для бакалавров	М.: Юрайт, 2011	21 экз.
2	Лебедев В. М., Ершов В. В.	Уголовно-процессуальное право: учеб. для студ. высш. учеб. заведений	М.: Юрайт, 2012	21 экз.
3	Кистяковский А. Ф.	Исследование о смертной казни	Санкт-Петербург: Лань, 2013	http://e.lanbook.com/books/element.php?p11_id=36402

5.2. Профессиональные базы данных и информационные справочные системы

Официальный интернет-портал правовой информации <http://pravo.gov.ru/>
 Гарант: Законодательство РФ, аналитика <http://www.garant.ru/>

5.3. Перечень программного обеспечения

Гарант (учебная версия)
 Libreoffice

5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-7: способен выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения			
З социальную значимость своей будущей профессии, обладает мотивацией к осуществлению профессиональной деятельности	осуществляет поиск и сбор необходимой литературы, использует различные базы данных, современные информационно-коммуникационные технологии и глобальные информационные ресурсы, в том числе правовые базы данных, дающие возможность рассмотреть общепризнанные принципы и нормы международного права, международные нормы и акты;	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет	Д - 4-6; ВЗ - 6-10;

<p>У выявлять проблемы в уголовном праве и находит пути их решения</p>	<p>выявляет проблемы, анализирует и использует различные источники информации для использования в своей профессиональной деятельности норм и актов уголовного права;</p>	<p>умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет</p>	<p>Т - Раздел 4: 16-34; Д - 4-6; ВЗ - 16, 17, 25-32;</p>
<p>В понятийно-категориальным аппаратом для осуществления своей профессиональной деятельности</p>	<p>выполняет задания, решает поставленные задачи, в соответствии с проблемой исследования, нормами уголовного права;</p>	<p>способность оценивать действия (бездействия) субъектов международного права, а также физических и юридических лиц государства, в соответствии с общепризнанными принципами и нормами международного права;</p>	<p>Т - Раздел 1: 1-2, Раздел 2: 3-10, Раздел 3: 11-15; Д - 4-6; ВЗ - 1-15;</p>
<p>ПК-4: способен юридически правильно квалифицировать факты и обстоятельства</p>			

<p>З уголовно- нормативно- правовые акты, регламентирующие правовой статус физических и юридических лиц, профессиональную деятельность юриста</p>	<p>осуществляет поиск и сбор необходимой литературы, использует различные базы данных, современные информационно- коммуникационные технологии и глобальные информационные ресурсы, в том числе правовые базы данных, дающие возможность рассмотреть уголовно- правовые нормы</p>	<p>соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет</p>	<p>ВЗ - 4-7; Д - 7-10,12;</p>
<p>У использовать юридическую терминологию, понимать общепризнанные понятия и категории в своей профессиональной деятельности;</p>	<p>использует визуальные средства в презентации (рисунки, диаграммы, графики и т.д.)</p>	<p>Визуальные средства хорошо координируются с содержанием и способствуют его пониманию.</p>	<p>ВЗ - 4-7; Д - 7-10,12;</p>
<p>В знаниями общепризнанной юридической терминологией, категориями и понятиями;</p>	<p>выступает перед аудиторией и доносит свою точку зрения в сфере уголовного права</p>	<p>уверенно выступает, удерживает внимание аудитории, формулирует и доносит до аудитории собственную позицию в сфере уголовно-правовой науки.</p>	<p>ВЗ - 4-7; Д - 7-10,12;</p>

ВЗ – вопрос к зачету;
Д – доклад.

1.2 Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

51-100 баллов (оценка «зачтено»)

0-50 баллов (оценка «не зачтено»).

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Понятие и признаки компьютерной информации.
 2. Понятие компьютерного преступления.
 3. Личностная характеристика преступника, совершившего компьютерные преступления.
 4. Основные опасные субъекты неправомерного доступа к компьютерной информации.
 5. Непосредственный объект компьютерного преступления.
 6. Основные направления обеспечения компьютерной безопасности.
 7. Понятие правового обеспечения компьютерной безопасности.
 8. Организационно-административные мероприятия.
 9. Организационно-технические мероприятия.
 10. Понятие способа совершения компьютерного преступления.
 11. Классификация способов совершения компьютерных преступлений.
 12. Понятие и классификация следов компьютерных преступлений.
 13. Регистрационные файлы операционных систем.
 14. Особенности подготовительного этапа осмотра места происшествия.
 15. Особенности криминалистического исследования компьютерных систем и их сетей на месте происшествия
 16. Криминалистическое исследование операционных систем.
 17. Сущность изъятия следов компьютерной информации.
 18. Фиксация следовой информации по делам о компьютерных преступлениях.
 19. Составление протокола изъятия следов компьютерных преступлений.
 20. Понятие и классификация компьютерно-технической экспертизы.
 21. Компьютерно-сетевая экспертиза.
 22. Комплексная компьютерно-техническая и технико-криминалистическая экспертиза.
 23. Угрозы безопасности информации.
 24. Средства защиты компьютерной информации.
 25. Методы защиты компьютерной информации.
 26. Основные мотивы при совершении компьютерных преступлений.
 27. Ответственность за неправомерный доступ к компьютерной информации.
 28. Ответственность за создание, использование и распространение вредоносных программ для ЭВМ.
 29. Ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
 30. Международный опыт борьбы с преступлениями в сфере компьютерной информации
- «зачтено» (51-100 баллов) выставляется студенту, обнаружившему знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой;
 - «не зачтено» (0-50 баллов) выставляется студенту, обнаружившему существенные пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий; давшему ответ, который не соответствует вопросу.

Темы докладов

1. Понятие и виды вредной информации.

2. Правовые проблемы борьбы со «спамом»
3. Классификация вредоносных программ и защита от их воздействия.
4. Информационная война.
5. Информационное оружие.
6. Кибертерроризм как новая угроза информационной безопасности.
7. Виды угроз компьютерной безопасности.
8. Электронные деньги: проблемы правового регулирования
9. Правовое регулирование информационных технологий в области электронной коммерции
10. Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
11. Правовое регулирование информационных технологий в области электронных банковских услуг
12. Правовое регулирование информационных технологий в области электронного документооборота
13. Стандартизация, сертификация и лицензирование в информационной сфере.
14. Информационные риски.

Критерии оценки:

оценка «отлично» (43-51 баллов) выставляется обучающемуся, если он перечисляет все существенные характеристики обозначенного в вопросе предмета и возможные варианты дальнейшего развития решения проблемы, если это возможно;

оценка «хорошо» (35-42 баллов), если студент раскрыл только часть основных положений вопроса, продемонстрировал неточность в представлениях о предмете вопроса;

оценка «удовлетворительно» (26-34 баллов), если студент обозначил общую траекторию ответа, но не смог конкретизировать основные компоненты;

оценка «неудовлетворительно» (0-25 баллов), если студент не продемонстрировал знаний основных понятий, представлений об изучаемом предмете.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Студент, не набравший минимального количества баллов, для получения зачета или не довольный количеством набранных баллов, выходит на промежуточную аттестацию.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по расписанию промежуточной аттестации в устном виде. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются вопросы международно-правового регулирования, правового статуса субъектов международного права, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки использования международно-правовых норм в своей профессиональной деятельности.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на все вопросы по изучаемой теме с использованием Libre Office..

По согласованию с преподавателем студент может подготовить доклад по теме занятия. В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях с использованием Libre Office..

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.

Методические рекомендации по написанию, требования к оформлению докладов

В целях расширения и закрепления полученных знаний при изучении данной дисциплины, студенту предлагается написание доклада. Тему доклада студент выбирает, исходя из круга научных интересов. Выполнение доклада преследует главную цель – использовать возможности активного, самостоятельного обучения в сочетании с другими формами учебных занятий и заданий по дисциплине.

Выполнение доклада позволяет решать следующие задачи обучения:

- глубже изучить отдельные темы учебной дисциплины;
- активизировать творческие способности учащихся, реализовать преимущества целенаправленной самоподготовки;
- позволяет дополнить текущий контроль знаний студентов;
- выработать навыки выполнения самостоятельной письменной работы, уметь работать с литературой, четко и последовательно выражать свои мысли.

Требования, предъявляемые к докладу:

- полное, глубокое и последовательное освещение темы;
- использование разнообразной литературы и материалов – учебных, статистических, нормативных, научных источников;
- ссылки на используемую литературу по тексту;

- самостоятельность изложения;
- аккуратность оформления работы;
- соблюдение установленных сроков написания и предоставления работы преподавателю.

Оформление доклада.

При написании доклада студенту следует соблюдать следующие требования к его оформлению:

1. Доклад выполняется с использованием Libre Office. на бумаге формата А4 машинописным способом: размер шрифта – 14 шрифт TimesNewRoman через полтора интервала; размер полей: левое – 30 мм, правое – 10 мм, верхнее и нижнее – 20 мм; нумерация страниц – в правом верхнем углу. Объем доклада: 10-15 листов.

2. Библиографические ссылки на использованные источники литературы при их цитировании рекомендуется оформлять подстрочными сносками. Цифровая нумерация подстрочных сносок начинается самостоятельно на каждом листе.

3. Каждая таблица, рисунок в докладе должны иметь сноску на источник литературы, из которого они заимствованы.

Структура доклада:

- титульный лист;
- лист содержания,
- основная часть работы,
- список использованной литературы,
- приложения.

Во введении указывается теоретическое и практическое значение темы и ее вопросов. Здесь также важно сформулировать цели и задачи, связанные с изучением и раскрытием темы, вкратце аргументировать план работы. Объем введения обычно не превышает 1 страницы.

В заключении приводятся основные, ключевые положения и выводы, которые вытекают из содержания работы. Весьма уместна и важна формулировка того, что дало вам изучение данной темы для накопления знаний по изучаемому курсу. Объем заключения может составлять до 2 страниц.

В списке использованной литературы источники приводятся в следующем порядке: сначала нормативно-правовые акты; затем научная, учебная литература, а также статьи из периодических изданий в алфавитном порядке с указанием полных выходных данных: фамилия и инициалы автора, название работы, место и год издания, название издательства; в конце списка приводятся официальные Интернет-ресурсы.