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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Киберпреступность и информационная безопасность

Направление 40.03.01 "Юриспруденция"
Направленность 40.03.01.02 "Гражданско-правовой профиль"

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Уголовное и уголовно-исполнительное право, криминология**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	10			
Вид занятий	УП	РП	УП	РП
Лекции	20	20	20	20
Практические	30	30	30	30
Итого ауд.	50	50	50	50
Контактная работа	50	50	50	50
Сам. работа	58	58	58	58
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.ю.н., доц., Дмитриев Д.Б.

Зав. кафедрой: д.ю.н., проф. Улезько С.И.

Методический совет направления: д.ю.н., профессор Позднышов А.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	- изучение теоретических и практических вопросов обеспечения информационной безопасности личности, общества и государства в новых технологических условиях, вопросов борьбы с киберпреступностью; - формирование у студентов навыков юридического сопровождения процессов, связанных с обеспечением информационной безопасности и противодействия киберпреступлениям.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

ОПК-8: Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

- методологию системного познания правовых явлений, процедуры критического анализа правовых явлений, содержание основных юридических понятий, категорий и конструкций;
- информационные источники получения юридически значимой информации, включая профессиональные базы данных;
- современные информационные технологии, которые используются в профессиональной деятельности юриста; (соотнесено с индикатором УК-1.1)
- требования информационной безопасности в сфере правоприменительной деятельности;
- методы работы с информационно-справочными системами для использования нормативных правовых документов в правоприменительной деятельности. (соотнесено с индикатором ОПК-8.1)

Уметь:

- осуществлять системный и критический анализ юридических понятий и категорий, выявлять системные взаимосвязи между отдельными правовыми понятиями и категориями;
- выделять необходимые источники информации, собирать информацию;
- получать из различных источников, включая правовые базы данных, юридически значимую информацию; (соотнесено с индикатором УК-1.2)
- использовать нормативные правовые документы в своей профессиональной деятельности юриста;
- решать задачи правоприменительной деятельности с использованием информационных технологий;
- решать задачи правоприменительной деятельности с учетом требований информационной безопасности. (соотнесено с индикатором ОПК-8.2)

Владеть:

- навыками использования инструментов системного и критического анализа правовых явлений, навыками принятия решений на основе данных о системной взаимосвязи юридических понятий, категорий и конструкций;
- навыками анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках и основными методами, способами и средствами получения, хранения, переработки правовой информации; (соотнесено с индикатором УК-1.3)
- навыками обработки и систематизации информации в соответствии с поставленной целью;
- основными приемами поиска документов в справочно-поисковых системах;
- навыками применения профессиональных баз данных и информационных технологий в правоприменительной деятельности;
- навыками обеспечения информационной безопасности своей правоприменительной деятельности. (соотнесено с индикатором ОПК-8.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. «Общая характеристика компьютерного оборота и компьютерной преступности»

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Тема 1.1. Научно-технический прогресс и его последствия (побочные эффекты). 1. Научно-техническая революция и социальное развитие. 2. Человек – компьютер – преступление. 3. Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны. / Лек /	8	2	УК-1, ОПК-8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.2	Тема 1.2. Основные законы и понятия современного информационного оборота. 1. Значение информации в жизни социума. 2. Правовое понятие и сущность компьютерной информации.	8	2	УК-1, ОПК-8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

	3. Основные подходы к определению понятия «компьютерная информация». 4. Основные нормативно-правовые акты регулирующие современный информационный оборот. 5. Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации. / Лек /				
1.3	Тема 1.3. Современная криминологическая оценка преступлений в сфере компьютерной информации. 1. Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации. 2. Латентность преступлений в сфере компьютерной информации. 3. Понятие сетевого компьютерного преступления. Типология сетевых компьютерных преступлений. 5. Использование основных понятий, категорий, институтов, правовых статусов субъектов уголовных правоотношений в криминологической оценке преступлений в сфере компьютерной информации. / Лек /	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.4	Тема 1.1. Научно-технический прогресс и его последствия (побочные эффекты). 1. Научно-техническая революция и социальное развитие. 2. Человек – компьютер – преступление. 3. Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны. / Пр /	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.5	Тема 1.2. Основные законы и понятия современного информационного оборота. 1. Значение информации в жизни социума. 2. Правовое понятие и сущность компьютерной информации. 3. Основные подходы к определению понятия «компьютерная информация». 4. Основные нормативно-правовые акты регулирующие современный информационный оборот. 5. Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации. / Пр /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.6	Тема 1.3. Современная криминологическая оценка преступлений в сфере компьютерной информации. 1. Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации. 2. Латентность преступлений в сфере компьютерной информации. 3. Понятие сетевого компьютерного преступления. Типология сетевых компьютерных преступлений. 5. Использование основных понятий, категорий, институтов, правовых статусов субъектов уголовных правоотношений в криминологической оценке преступлений в сфере компьютерной информации. / Пр /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

Раздел 2. «Правовые основы борьбы с компьютерной преступностью и компьютерными преступлениями»

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Тема 2.1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ. 1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК). 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК). 4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК). 5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

	телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). / Лек /				
2.2	Тема 2.2. Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации. 1. Мошенничество в сфере компьютерной информации. 2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 3. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. 4. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. 5. Составы преступлений, содержащие квалифицирующий признак “с использованием информационно-телекоммуникационных сетей” / Лек /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.3	Тема 2.3. Вопросы квалификации преступлений в сфере компьютерной информации. 1. Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений 2. Место совершения преступлений в сфере компьютерной информации 3. Отдельные проблемные вопросы, связанные с моментом окончания преступлений в сфере компьютерной информации. / Лек /	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.4	Тема 2.4. Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации. 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. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран. 4. Сравнительно-правовой анализ отдельных преступлений в сфере компьютерной информации в зарубежном уголовном законодательстве 5. Международные соглашения в сфере борьбы с компьютерными преступлениями. Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ. 6. Подходы различных государств к уголовно - правовому регулированию борьбы с преступлениями в глобальных компьютерных сетях. / Лек /	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.5	Тема 2.5. Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника. 1. Причины и условия преступлений в сфере компьютерной информации. 2. Особенности личности преступника в сфере компьютерной информации. 3. Типология личности преступника в сфере компьютерной информации. 4. Особенности лиц, совершающих преступления в глобальных компьютерных сетях. / Лек /	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.6	Тема 2.6. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ. 1. Основные направления профилактики преступлений в сфере компьютерной информации. 2. Правовое регулирование борьбы с преступлениями в сфере компьютерной информации. 3. Меры предупреждения преступлений в сфере компьютерной информации. 4. Виктимологическая профилактика преступлений в сфере компьютерной информации.	8	2	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

	5. Система субъектов, осуществляющих борьбу с преступлениями в сфере компьютерной информации. 6. Особенности предупреждения преступлений в глобальных компьютерных сетях. / Лек /				
2.7	Тема 2.1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ. 1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК). 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК). 4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК). 5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). / Пр /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.8	Тема 2.2. Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации. 1. Мошенничество в сфере компьютерной информации. 2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 3. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. 4. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. 5. Составы преступлений, содержащие квалифицирующий признак “с использованием информационно-телекоммуникационных сетей” / Пр /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.9	Тема 2.3. Вопросы квалификации преступлений в сфере компьютерной информации. 1. Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений 2. Место совершения преступлений в сфере компьютерной информации 3. Отдельные проблемные вопросы, связанные с моментом окончания преступлений в сфере компьютерной информации. / Пр /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.10	Тема 2.4. Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации. 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. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран. 4. Сравнительно-правовой анализ отдельных преступлений в сфере компьютерной информации в зарубежном уголовном законодательстве 5. Международные соглашения в сфере борьбы с компьютерными преступлениями. Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ. 6. Подходы различных государств к уголовно - правовому регулированию борьбы с преступлениями в глобальных компьютерных сетях. / Пр /	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.11	Тема 2.5. Причины и условия преступлений в сфере компьютерной информации. Особенности личности	8	4	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

	компьютерного преступника. 1. Причины и условия преступлений в сфере компьютерной информации. 2. Особенности личности преступника в сфере компьютерной информации. 3. Типология личности преступника в сфере компьютерной информации. 4. Особенности лиц, совершающих преступления в глобальных компьютерных сетях. / Пр /				
2.12	Тема 2.6. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ. 1. Основные направления профилактики преступлений в сфере компьютерной информации. 2. Правовое регулирование борьбы с преступлениями в сфере компьютерной информации. 3. Меры предупреждения преступлений в сфере компьютерной информации. 4. Виктимологическая профилактика преступлений в сфере компьютерной информации. 5. Система субъектов, осуществляющих борьбу с преступлениями в сфере компьютерной информации. 6. Особенности предупреждения преступлений в глобальных компьютерных сетях. / Ср /	8	58	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.13	/ Зачёт /	8	0	УК-1, ОПК -8	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Степанов-Егиянц В. Г.	Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография	Москва: Статут, 2016	https://biblioclub.ru/index.php?page=book&id=452481 неограниченный доступ для зарегистрированных пользователей
Л1.2	Корабельников, С. М.	Преступления в сфере информационных отношений: учебное пособие	Москва: Всероссийский государственный университет юстиции (РПА Минюста России), 2015	https://www.iprbookshop.ru/43237.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Борисов С.	Преступления в сфере компьютерной информации: монография	Москва: Лаборатория книги, 2010	https://biblioclub.ru/index.php?page=book&id=101046 неограниченный доступ для зарегистрированных пользователей
Л2.2	Милашевская Е. С.	Уголовная ответственность за преступления в сфере компьютерной информации: монография	Москва: Лаборатория книги, 2012	https://biblioclub.ru/index.php?page=book&id=142535 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.3		Lex russica (Русский закон)	, 2004	https://www.iprbookshop.ru/63405.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ИСС «КонсультантПлюс»
ИСС «Гарант» http://www.internet.garant.ru/
База данных Генеральной прокуратуры РФ. Портал правовой статистики http://crimestat.ru/
База данных Федеральной службы государственной статистики РФ http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/infraction/
База данных МВД РФ https://мвд.рф/
База данных Генеральной прокуратуры РФ https://genproc.gov.ru/
База данных Судебного департамента при ВС РФ http://www.supcourt.ru/index.php/

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.5. Учебно-методические материалы для студентов 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.

Приложение 1

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
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач			
Знать: - методологию системного познания правовых явлений, процедуры критического анализа правовых явлений, содержание основных юридических понятий, категорий и конструкций; - информационные источники получения юридически значимой информации, включая профессиональные базы данных; - современные информационные технологии, которые используются в профессиональной деятельности юриста;	- осуществляет поиск и сбор необходимой литературы и примеров судебной практики при подготовке к докладу; - информирует аудиторию, дает исчерпывающие ответы на заданные вопросы; - выполняет тестовые задания. - отвечает на основные и дополнительные вопросы, вынесенные на зачет.	- целенаправленность поиска и отбора информации; - полнота и содержательность доклада, ответа на вопрос к зачету; - соответствие представленной студентом информации существующим законодательным актам, реальной судебной практике, материалам лекций и учебной литературы; - верность ответа на тестовые задания (в полном, не полном объеме).	Д – доклады (Раздел 1:1.1.-1.3., Раздел 2: 2.1.-2.5.); Т–тесты (Раздел 1:1.1.-1.3., Раздел 2: 2.1.-2.6.); вопросы к зачету (1-25).
Уметь: - осуществлять системный и критический анализ юридических понятий и категорий, выявлять системные взаимосвязи между отдельными правовыми понятиями и категориями; - выделять необходимые источники информации, собирать информацию; - получать из различных источников, включая правовые базы данных, юридически значимую информацию;	- подбирает литературу и примеры судебной практики, необходимые для написания эссе; - успешно выполняет практико-ориентированные задания для самостоятельной работы.	- целенаправленность поиска и отбора информации для написания эссе, соответствие отобранной информации существующим законодательным актам, реальной судебной практике, материалам лекций и учебной литературы; - выполнение практико-ориентированных заданий в соответствии с действующими нормативно-правовыми актами и реальной судебной практикой; - объем выполненных заданий для самостоятельной работы (в полном, не полном объеме).	ЭС – эссе (темы 1-30); практико-ориентированные задания (1-15).

Владеть: - навыками использования инструментов системного и критического анализа правовых явлений, навыками принятия решений на основе данных о системной взаимосвязи юридических понятий, категорий и конструкций; - навыками анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках и основными методами, способами и средствами получения, хранения, переработки правовой информации;	- выполняет кейс-задание с аргументацией полученного результата; - успешно выполняет практико-ориентированные задания для самостоятельной работы.	- студент правильно выполняет кейс-задания/ практико-ориентированные задания в соответствии с действующим законодательством и реальной судебной практикой, обоснованно аргументирует полученный результат, демонстрируя наличие твердых и достаточно полных знаний в решении поставленных перед ним задач; - объем выполненного задания (в полном, не полном объеме).	КЗ – кейс-задача (1-9); практико-ориентированные задания (1-15).
ОПК-8: Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности			
Знать: - требования информационной безопасности в сфере правоприменительной деятельности; - методы работы с информационно-справочными системами для использования нормативных правовых документов в правоприменительной деятельности.	- осуществляет поиск и сбор необходимой литературы и примеров судебной практики при подготовке к докладу; - информирует аудиторию, дает исчерпывающие ответы на заданные вопросы; - выполняет тестовые задания. - отвечает на основные и дополнительные вопросы вынесенные на зачет.	- целенаправленность поиска и отбора информации; - полнота и содержательность доклада, ответа на вопрос к зачету; - соответствие представленной студентом информации существующим законодательным актам, реальной судебной практике, материалам лекций и учебной литературы; - верность ответа на тестовые задания (в полном, не полном объеме).	Д – доклады (Раздел 1:1.1.-1.3., Раздел 2: 2.1.-2.5.); Т–тесты (Раздел 1:1.1.-1.3., Раздел 2: 2.1.-2.6.); вопросы к зачету (1-25).

Уметь: - использовать нормативные правовые документы в своей профессиональной деятельности юриста; - решать задачи правоприменительной деятельности с использованием информационных технологий; - решать задачи правоприменительной деятельности с учетом требований информационной безопасности.	- подбирает литературу и примеры судебной практики, необходимые для написания эссе; - успешно выполняет практико-ориентированные задания для самостоятельной работы.	- целенаправленность поиска и отбора информации для написания эссе, соответствие отобранной информации существующим законодательным актам, реальной судебной практике, материалам лекций и учебной литературы; - выполнение практико-ориентированных заданий в соответствии с действующими нормативно-правовыми актами и реальной судебной практикой; - объем выполненных заданий для самостоятельной работы (в полном, не полном объеме).	ЭС – эссе (темы 1-30); практико-ориентированные задания (1-15).
Владеть: - навыками обработки и систематизации информации в соответствии с поставленной целью; - основными приемами поиска документов в справочно-поисковых системах; - навыками применения профессиональных баз данных и информационных технологий в правоприменительной деятельности; - навыками обеспечения информационной безопасности своей правоприменительной деятельности.	- выполняет кейс-задание с аргументацией полученного результата; - успешно выполняет практико-ориентированные задания для самостоятельной работы.	- студент правильно выполняет кейс-задания/ практико-ориентированные задания в соответствии с действующим законодательством и реальной судебной практикой, обоснованно аргументирует полученный результат, демонстрируя наличие твердых и достаточно полных знаний в решении поставленных перед ним задач; - объем выполненного задания (в полном, не полном объеме).	КЗ – кейс-задача (1-9); практико-ориентированные задания (1-15).

1.2 Шкалы оценивания:
Зачет:
Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно–рейтинговой системы в 100–балльной шкале:
50-100 баллов – оценка «зачтено»;
0-49 баллов – оценка «не зачтено».

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

Вопросы к зачету:
1. Развитие техники как прогресс и источник социальных проблем.
2. Влияние НТП на соотношение умышленной и неосторожной преступности.
3. Возможности и пределы влияния уголовного законодательства на технический прогресс.
4. Значение информации в жизни социума.
5. Компьютерная форма информации, ее достоинства и проблемы пользования. Свобода и ограничения в пользовании информацией.
6. Понятийный ряд электронного (компьютерного) оборота.
7. Нормативная основа, регулирующая оборот компьютерной информации в современном обществе.

8. Информация как очевидный объект криминальных посягательств.
9. Хакерские атаки и компьютерные вирусы.
10. Криминологическая характеристика современной компьютерной преступности в России и за рубежом.
11. Основной состав преступления в виде неправомерного доступа к компьютерной информации (ст.272 УК РФ).
12. Можно ли считать компьютерную информацию предметом преступления, а компьютерные посягательства относить к категории материальных составов?
13. Значение примечаний к ст. 272 УК РФ.
14. Понятие вредоносных компьютерных программ и способы их распространения (ст.273 УК РФ).
15. «Материальность» состава и виды обязательных последствий (уничтожение, блокирование, модификация, копирование или нейтрализация средств защиты компьютерной информации) (ст.273 УК РФ).
16. Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ (ст.273 УК РФ).
17. Характеристика квалифицирующих признаков состава преступления "Создание, использование и распространение вредоносных компьютерных программ" (ст.273 УК РФ).
18. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст.274 УК РФ).
19. Уголовно-правовая характеристика ст. 274.1 УК РФ "Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации".
20. Уголовно-правовая характеристика ст. 274.2 УК РФ "Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования".
21. Бланкетная основа уголовной ответственности за компьютерное преступление.
22. Понятие информационно-телекоммуникационных сетей.
23. Причины и условия как детерминанты преступности.
24. Личность компьютерного преступника.
25. Предупреждение компьютерной преступности и профилактика компьютерных преступлений.

Зачетное задание состоит из двух теоретических вопросов и одного практико-ориентированного задания.

Практико-ориентированные задания

Задание №1.
Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема — одного из элементов компьютерной системы.
Вопросы:
Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

Задание №2.
Бережной заказал знакомому программисту Пятеркину написать программу, находящую и расширяющую бреши в защите персональных компьютеров и информационно-телекоммуникационных сетей. С ее помощью Бережной проник в сеть банка «Капитал» и уничтожил всю информацию о предоставлении ему кредита в размере 1,5 млн рублей.
Вопросы:
1. По какой статье (части статьи) УК РФ следует квалифицировать действия Бережного.
2. Раскрыть: Объект, Объективную сторону, Субъект, Субъективную сторону.

Задание №3.
Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации. Внутренняя проверка факт неправомерного доступа подтвердила.
Вопросы:
1. Какая статья уголовного кодекса подлежит применению?

2. Какое наказание должен понести нарушитель?

Задание №4.
Руководитель отдела информационной безопасности организации установил, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.
Вопросы:
1. Какая статья уголовного кодекса подлежит применению?
2. Какое наказание должен понести нарушитель?

Задание №5.
Гражданин П. проник в информационную базу государственного учреждения и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.
Вопросы:
1. Являются ли его действия противозаконными?
2. С чем это связано?
3. Какое наказание может ждать гражданина П. за совершенные им действия?

Задание №6.
Гражданин С. являясь администратором автоматизированной информационно-поисковой системы (АИПС), как инженер-программист регионального отдела информационного обеспечения, наделенный высшим уровнем доступа в Сеть, произвел незаконные уничтожение охраняемой законом служебной информации о совершении рядом лиц административных правонарушений и лишении их права управления транспортными средствами.
Вопрос:
Как следует квалифицировать содеянное С.

Задание №7.
К., находясь у себя дома, имея свободный доступ к сети Интернет, используя кабель для сети Интернет, ноутбук «DELL», осуществил соединение с сервером собственника информационных ресурсов «Филиал в г. Барнауле ЗАО «ЭР-Телеком Холдинг», предоставляющего услуги доступа к компьютерной сети Интернет, в сети Интернет зашёл на электронный ресурс ООО «Мэйл.ру», после чего, незаконно используя учетную запись в виде логина «Iarantl972@mail.ru», принадлежащего А., ввел его в поле «Логин», а затем, воспользовавшись системой восстановления пароля через ключевое слово, в поле «секретный вопрос - больница», ввел слово «краевая», а в строке «пароль» ввел новый пароль «12345g». После чего, К., активировал клавишу «войти» и тем, самым совершил неправомерный доступ к электронному почтовому ящику «Iarantl972@mail.ru», принадлежащему А, что повлекло модификацию компьютерной информации на электронном почтовом ящике А. и сервере собственника информационных ресурсов ООО «Мэйл.ру», то есть, изменение ее содержания по сравнению с той информацией, которая первоначально была в распоряжении собственника информации и, поменяв пароль, заблокировал её, то есть создал условия невозможности использования информации собственником при её сохранности.
Вопрос:
Как следует квалифицировать содеянное К.

Задание №8.
Ш., Л., П., Щ. посредством сети Интернет приобрели у неустановленного лица техническое устройство «скиммер». Затем, используя подручные средства, совместными усилиями во фрагмент пластиковой трубы, обернутый фольгой, поместили видеокамеру с носителем информации и иные детали, изъятые из приобретенного для этой цели видеорегистратора, и привели их в рабочее состояние, тем самым изготовили самодельное техническое устройство «планка», предназначенное для установки на корпус банкомата, непосредственно над клавиатурой, с целью видеофиксации цифровых символов ПИН-кодов к банковским картам граждан. После чего Ш., Л., П., Щ. совместно подыскали банкомат конструктивно подходящий для установки технических устройств «скиммер» и «планка» и установили их. Во время работы указанных технических устройств, при самообслуживании в банкомате потерпевшие производили операции с личными банковскими картами. В результате этого Ш., Л., П., Щ с помощью технического устройства «скиммер» при прохождении через него банковских карт с их магнитных полос производилось считывание и копирование информации об индивидуальных цифровых свойствах банковских карт на встроенный носитель информации, а также с помощью технического устройства «планка» со скрытой видеокамерой и носителем информации была произведена видеофиксация последовательности набора данными клиентами на клавиатуре банкомата цифровых символов ПИН-кодов с сохранением указанных видеоданных. После чего установленные технические устройства демонтировались. Таким образом, Ш., Л., П., Щ осуществили неправомерный доступ к содержащейся на магнитных полосах информации об индивидуальных цифровых свойствах банковских

карт, и, кроме того, в электронную память технических устройств, установленных подсудимыми, были скопированы сведения об индивидуальных цифровых свойствах банковских карт. Впоследствии Ш., Л., П., Щ преобразовывали данную информацию с помощью компьютера, делая ее пригодной для последующей записи на магнитные полосы новых пластиковых карт. Таким образом, были изготовлены дубликаты пластиковых карт. После чего Ш., сопоставив по времени и последовательности фиксации информацию, полученную с помощью технического устройства «скиммер», с информацией, полученной с помощью технического устройства «планка», определял цифровые символы ПИН-кода доступа к счету законного владельца каждой банковской карты и записывал их на отдельный лист в последовательности, соответствующей раскладке дубликатов банковских карт. Впоследствии с помощью дубликатов банковских карт и полученных сведений о пин-кодах Ш., Л., П., Щ произвели операции по снятию денежных средств.
Вопросы:
Что понимается под копированием информации?
Что будет инкриминировано Ш., Л., П., Щ.?

Задание №9.
Знакомый похитил расчетную пластиковую карту знакомого. Завладел денежной суммой в размере 5000 рублей. Следователь сказал, что будет предъявлено обвинение по ст. 272 УК РФ.
Вопрос:
Имеется ли указанный состав преступления?

Задание №10.
Сотрудник административных сетей организации в личных интересах «майнил» криптовалюту, не обновил защитную систему, допустил причинение вреда инфраструктуре.
Вопрос:
Квалифицируйте содеянное.

Задание №11.
Системный администратор учреждения при работе не использовал систему безопасности. В результате было осуществлено копирование информации с персональными данными сотрудников и личными контактами коммерческих партнеров, что причинило учредению крупный ущерб. Уголовное дело было ошибочно возбуждено по ст. 272 УК РФ и передано в суд. Постановленный судебный приговор был отменен надзорной инстанцией, уголовное дело прекращено, по обстоятельствам истечения сроков привлечения к уголовной ответственности. Следственные и судебные органы не учли, что преступление совершил специальный субъект - законный пользователь.
Вопрос:
По какой статье (части статьи) уголовного закона следовало квалифицировать деяние.

Задание №12.
Судом установлено, что с марта по апрель этого года студент К. с домашнего компьютера произвел ряд DDoS-атак (распределенных атак типа "отказ в обслуживании") на компьютерную информацию, хранящуюся на ресурсах сайтов ЗАО Банк "Тиньк", ЗАО "Лаборатория Каспера", ОАО "Промвязьбанк" и ЗАО "Издательский дом "Комсомольская неправда".
В итоге была блокирована работа этих сайтов, в том числе личных кабинетов пользователей интернет-банка, мобильных банка и кошелька, систем СМС-информирования, POS-терминалов в интернете, продажа продуктов на сайтах, а также системы авторизации и офисного интернета – Wi-Fi.
24 марта студент К. в одной из соцсетей потребовал от владельца банка "ТКС" $1000 за прекращение DDoS-атаки. Когда же банкир отказался платить и пригрозил хакеру уголовной ответственностью, тот увеличил требуемую сумму до $3000.
Вскоре Кузьмин был задержан сотрудниками полиции. Общий ущерб, причиненный им правообладателям, превысил 11 млн руб.
Вопрос:
По каким статьям уголовного закона Кузьмин будет признан судом виновным?

Задание №13.
Солдатова в начале декабря 2016 года в вечернее время находилась в квартире знакомой Мещеряковой с малознакомой Рахмановой. Рахманова, ложась спать, разрешила ей пользоваться своим сотовым телефоном. Увидев, что на телефон Рахмановой пришло смс - сообщение о поступлении денег на карту она решила похитить данные денежные средства со счета карты. С телефона Рахмановой набрала команду перевод с карты на карту, указав номер карты, оформленной на ее имя, сумму перевода. Дважды она перевела по 4000 рублей на свою карту, приходящие смс- сообщения о списании денежных средств она удаляла. После перевода денег она ушла, из квартиры, сняла со своей карты денежные средства в сумме 8000 рублей, которые потратила на личные нужды.

Вопрос:
Какое преступление совершила Солдатова?

Задание №14.
Сотрудник организации, по специальности программист, разработал антивирусную программу. С целью продолжения работы (на период отпуска) забрал копию на флеш-карте домой. Его ребенок без разрешения взял носитель информации, запустил вирус в сеть на уроке информатики. Из-за этого был причинен вред электронной системе образовательного учреждения.
Вопрос:
Какая ответственность грозит программисту?

Задание №15.
Иванов, работая в организации связи, подсмотрел данные для входа в специальную систему, ознакомился с детализацией звонков невесты.
Вопросы:
Усматривается ли в действиях Иванова состав преступления?

Критерии оценивания:
- оценка «зачтено» (50-100 баллов) выставляется студенту, если ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов.
- оценка «не зачтено» (0-49 баллов) материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине.

Вопросы для докладов

Раздел 1. «Общая характеристика компьютерного оборота и компьютерной преступности»
Тема 1.1. Научно-технический прогресс и его последствия (побочные эффекты).
1. Научно-техническая революция и социальное развитие.
2. Человек – компьютер – преступление.
3. Возможности и пределы влияния уголовного законодательства на технический прогресс и на его изъяны.

Тема 1.2. Основные законы и понятия современного информационного оборота.
1. Значение информации в жизни социума.
2. Правовое понятие и сущность компьютерной информации.
3. Основные подходы к определению понятия «компьютерная информация».
4. Основные нормативно-правовые акты регулирующие современный информационный оборот.
5. Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации.

Тема 1.3. Современная криминологическая оценка преступлений в сфере компьютерной информации.
1. Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации.
2. Латентность преступлений в сфере компьютерной информации.
3. Понятие сетевого компьютерного преступления. Типология сетевых компьютерных преступлений.
4. Использование основных понятий, категорий, институтов, правовых статусов субъектов уголовных правоотношений в криминологической оценке преступлений в сфере компьютерной информации.

Раздел 2. «Правовые основы борьбы с компьютерной преступностью и компьютерными преступлениями»
Тема 2.1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ.
1. Неправомерный доступ к компьютерной информации (ст. 272 УК).
2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).
4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).
5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК).

Тема 2.2. Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации

1. Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений
2. Место совершения преступлений в сфере компьютерной информации
3. Отдельные проблемные вопросы, связанные с моментом окончания преступлений в сфере компьютерной информации.

Тема 2.3. Вопросы квалификации преступлений в сфере компьютерной информации..
1. Мошенничество в сфере компьютерной информации.
2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.
3. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.
4. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем.
5. Составы преступлений, содержащие квалифицирующий признак “с использованием информационно-телекоммуникационных сетей”

Тема 2.4. Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации.
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. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.
4. Сравнительно-правовой анализ отдельных преступлений в сфере компьютерной информации в зарубежном уголовном законодательстве
5. Международные соглашения в сфере борьбы с компьютерными преступлениями. Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ.
6. Подходы различных государств к уголовно - правовому регулированию борьбы с преступлениями в глобальных компьютерных сетях.

Тема 2.5. Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника.
1. Причины и условия преступлений в сфере компьютерной информации.
2. Особенности личности преступника в сфере компьютерной информации.
3. Типология личности преступника в сфере компьютерной информации.
4. Особенности лиц, совершающих преступления в глобальных компьютерных сетях.

Тема 2.6. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.
1. Основные направления профилактики преступлений в сфере компьютерной информации.
2. Правовое регулирование борьбы с преступлениями в сфере компьютерной информации.
3. Меры предупреждения преступлений в сфере компьютерной информации.
4. Виктимологическая профилактика преступлений в сфере компьютерной информации.
5. Система субъектов, осуществляющих борьбу с преступлениями в сфере компьютерной информации.
6. Особенности предупреждения преступлений в глобальных компьютерных сетях.

Критерии оценивания:
27 бальная оценка: ответы по каждой теме оцениваются максимум в 3 балла.
3 балла - обучающийся выделяет главные положения в изученном материале и не затрудняется при изложении материала, отвечает на видоизмененные вопросы, свободно применяет полученные знания на практике, не допускает ошибок в воспроизведении изученного материала;
2 балла - обучающийся владеет изученным материалом, отвечает без особых затруднений на вопросы преподавателя, умеет применять полученные знания на практике, в устных ответах не допускает серьезных ошибок, легко устраняет отдельные неточности с помощью дополнительных вопросов преподавателя;
1 балл – обучающийся усвоил основной материал, но испытывает затруднение при его самостоятельном воспроизведении и требует дополнительных и уточняющих вопросов преподавателя, испытывает затруднение при ответах на дополнительные вопросы;
0 баллов - имеются отдельные представления об изученном материале, но все же большая часть материала не усвоена, при ответе на вопросы допускает грубые ошибки.

Кейс-задача

Раздел 1. «Общая характеристика компьютерного оборота и компьютерной преступности»
Тема 1.1. Научно-технический прогресс и его последствия (побочные эффекты).
Кейс-задача № 1
1. Подберите и перечислите источники информации, имеющие отношение к теме 1.1.
2. Составьте глоссарий к теме 1.1.
3. Составьте 10 ситуационных задач по теме 1.1 и приведите их решение.

Тема 1.2. Основные законы и понятия современного информационного оборота.
Кейс-задача № 2
1. Подберите и перечислите источники информации, имеющие отношение к теме 1.2.
2. Составьте глоссарий к теме 1.2.
3. Составьте 10 ситуационных задач по теме 1.2 и приведите их решение.

Тема 1.3. Современная криминологическая оценка преступлений в сфере компьютерной информации.
Кейс-задача № 3
1. Подберите и перечислите источники информации, имеющие отношение к теме 1.3.
2. Составьте глоссарий к теме 1.3.
3. Составьте 10 ситуационных задач по теме 1.3 и приведите их решение.

Раздел 2. «Правовые основы борьбы с компьютерной преступностью и компьютерными преступлениями»
Тема 2.1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ.
Кейс-задача № 4
1. Подберите и перечислите источники информации, имеющие отношение к теме 2.1.
2. Составьте глоссарий к теме 2.1.
3. Составьте 10 ситуационных задач по теме 2.1 и приведите их решение.

Тема 2.2. Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации Кейс-задача № 5
1. Подберите и перечислите источники информации, имеющие отношение к теме 2.2.
2. Составьте глоссарий к теме 2.2.
3. Составьте 10 ситуационных задач по теме 2.2 и приведите их решение.

Тема 2.3. Вопросы квалификации преступлений в сфере компьютерной информации.
Кейс-задача № 6
1. Подберите и перечислите источники информации, имеющие отношение к теме 2.3.
2. Составьте глоссарий к теме 2.3.
3. Составьте 10 ситуационных задач по теме 2.3 и приведите их решение.

Тема 2.4. Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации.
Кейс-задача № 7
1. Подберите и перечислите источники информации, имеющие отношение к теме 2.4.
2. Составьте глоссарий к теме 2.4.
3. Составьте 10 ситуационных задач по теме 2.4 и приведите их решение.

Тема 2.5. Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника.
Кейс-задача № 8
1. Подберите и перечислите источники информации, имеющие отношение к теме 2.5.
2. Составьте глоссарий к теме 2.5.
3. Составьте 10 ситуационных задач по теме 2.5 и приведите их решение.

Тема 2.6. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.
Кейс-задача № 9
1. Подберите и перечислите источники информации, имеющие отношение к теме 2.6.
2. Составьте глоссарий к теме 2.6.
3. Составьте 10 ситуационных задач по теме 2.6 и приведите их решение.

Критерии оценивания:
27 бальная: каждая кейс-задача оценивается максимум в 3 балла.
3 балла - кейс-задача решено правильно, дано развернутое пояснение и обоснование сделанного заключения. Студент демонстрирует методологические и теоретические знания, свободно владеет научной терминологией. При разборе предложенной ситуации проявляет творческие способности, знание дополнительной литературы. Демонстрирует хорошие аналитические способности, способен при обосновании своего мнения свободно проводить аналогии между темами дисциплины;
2 балла - кейс-задача решено правильно, дано пояснение и обоснование сделанного заключения. Студент демонстрирует методологические и теоретические знания, свободно владеет научной терминологией. Демонстрирует хорошие аналитические способности, однако допускает некоторые неточности при оперировании научной терминологией.
1 балл - кейс-задача решено, пояснение и обоснование сделанного заключения было дано при активной помощи преподавателя. Студент имеет ограниченные теоретические знания, допускает существенные ошибки при установлении логических взаимосвязей, допускает ошибки при использовании научной терминологии.
0 баллов - кейс-задача решено неправильно, обсуждение и помощь преподавателя не привели к правильному заключению. Студент обнаруживает неспособность к построению самостоятельных заключений. Имеет слабые теоретические знания, не использует научную терминологию.

Темы эссе

1. Проблемы криминализации деяний в сфере компьютерной информации.
2. Сравнительный анализ российского и зарубежного уголовного законодательства о преступлениях в сфере компьютерной безопасности.
3. Спорные вопросы объективной стороны преступлений в сфере компьютерной информации.
4. Влияние компьютерной техники и информационных технологий на развитие уголовного права России.
5. Вредоносная программа как предмет преступления.
6. Криминологическая характеристика преступлений в сфере компьютерной информации.
7. Анализ воздействия киберпреступности на финансовый и иные сектора экономики.
8. Взаимодействие компьютерной и организованной преступности.
9. Виды и классификация преступлений совершаемых с использованием компьютерных технологий.
10. Перспективные направления совершенствования уголовного законодательства об ответственности за преступления в сфере компьютерной информации.
11. Причины и условия преступлений в сфере компьютерной информации в историческом аспекте.
12. Криминологическая характеристика личности преступника в сфере компьютерной информации.
13. Особенности личности преступника, совершающего преступления в глобальных компьютерных сетях.
14. Борьба с компьютерной преступностью: организационные, правовые и методические аспекты.
15. Перспективы совершенствование системы борьбы с киберпреступностью.
16. Место и роль правовых средств в профилактике компьютерных преступлений.
17. Международное сотрудничество в борьбе с киберпреступностью.
18. Вредоносные программы как средство информационной войны.
19. История вредоносных программ.
20. Информационные отношения как предмет правового регулирования.
21. Понятие и структура информационной безопасности как объекта уголовно - правовой охраны.
22. Информация как предмет преступлений против информационной безопасности.
23. Законодательство РФ в области обеспечения информационной безопасности.
24. Общая характеристика и виды преступлений информационной безопасности по уголовному законодательству зарубежных стран.
25. Проблемы квалификации иных преступлений против информационной безопасности.
26. Проблемы квалификации преступлений, совершаемых с использованием глобальных компьютерных сетей (сети Интернет).
27. Проблемы квалификации преступлений в сфере компьютерной информации по объекту (предмету) и объективной стороне.
28. Проблемы квалификации преступлений в сфере компьютерной информации по субъективной стороне и субъекту.
29. Квалифицированные виды преступлений в сфере компьютерной информации и их уголовно – правовая оценка.
30. Перспективные направления совершенствования уголовного законодательства об ответственности за преступления против информационной безопасности.

Критерии оценивания:
Студент за семестр готовит одно эссе по предложенным темам. Максимальный балл – 36.

30-36 баллов – блестящая работа, которая отвечает всем предъявляемым требованиям, а также отличается научной новизной и является вкладом в развитие правовой науки.
22-29 баллов – эссе соответствует всем требованиям, предъявляемым к такого рода работам. Тема эссе раскрыта полностью, четко выражена авторская позиция, имеются логичные и обоснованные выводы. Эссе написано с использованием большого количества нормативных правовых актов на основе рекомендованной основной и дополнительной литературы. На высоком уровне выполнено оформление работы, использована программа Microsoft PowerPoint.
14-21 баллов – тема эссе раскрыта полностью; прослеживается авторская позиция, сформулированы необходимые обоснованные выводы; использована необходимая для раскрытия вопроса основная и дополнительная литература и нормативные правовые акты. Грамотное оформление.
6-13 баллов – в целом тема эссе раскрыта; выводы сформулированы, но недостаточно обоснованы; имеется анализ необходимых правовых норм, со ссылками на необходимые нормативные правовые акты; использована необходимая как основная, так и дополнительная литература; недостаточно четко проявляется авторская позиция.
1-5 баллов – тема раскрывается на основе использования нескольких основных и дополнительных источников; слабо отражена собственная позиция, выводы имеются, но они не обоснованы; материал изложен непоследовательно, без соответствующей аргументации и анализа правовых норм, хотя ссылки на нормативные правовые акты встречаются. Имеются недостатки по оформлению
0 баллов – выставляется обучающемуся, если материал не раскрывает тему, при ответе выявлено непонимание сущности излагаемого вопроса, неуверенность и неточность при ответах на вопросы. Работа имеет незаконченный, несамостоятельный характер, присутствует плагиат.

Тесты

Банк тестов (с различными типами) по разделам и/или по темам
● - закрытые тесты с одним правильным ответом - необходимо выбрать из предложенных вариантов только один правильный ответ.
■ - закрытые тесты с двумя и более правильными ответами - необходимо выбрать не менее двух правильных ответов из предложенных вариантов.

Раздел 1. «Общая характеристика компьютерного оборота и компьютерной преступности»
Тема 1.1. Научно-технический прогресс и его последствия (побочные эффекты)
■ 1. Основные этапы НТП:
- доиндустриальный
- постиндустриальный
- эволюционный
- современный

■ 2. Характер распространения достижений НТП:
- глобальный
- локальный
- скачкообразный
- волнообразный

● 3. Коренное преобразование производительных сил на основе превращения науки в ведущий фактор развития производства, непосредственную производительную силу называется:
- научно-технической революцией
- научно-техническим прогрессом
- технологическим детерминизмом
- производством высоких технологий

■ 4. Первый этап научно-технической революции базировался на развитии следующих основных направлений:
- освоении энергии атома
- кибернетике и вычислительной технике
- информатики
- квантовой электронике и лазерной технике

● 5. С конца 70-х гг. XX в. начался новый этап научно-технической революции, получивший название
- полиструктурной
- автоматизации производственных процессов
- квантовой революции
- революции робототехники

● 6. Первым человеком, использовавшим возможности электронно-вычислительной машины для совершения налогового преступления считался
- Альфонсе Конфессоре
- Кевин Митник
- Гэри Маккиннон
- Адриан Ламо

● 7. Общей чертой современной НТР является:
- всеохватность
- чрезвычайное ускорение научно-технических преобразований
- качественно новая роль человека в процессе производства
- сохранение военно-технического характера
- все варианты ответов верны

■ 8. Второй этап научно-технической революции связывают с развитием:
- информатики
- биотехнологии
- микроэлектроники
- кибернетики и вычислительной техники

● 9. Теория, предполагающая постепенный переход государственного управления в руки инженерно-технической интеллигенции
- технократизм
- эссенциализм
- энергетизм
- социализм

● 10. Главный путь развития в эпоху НТР техники и технологии:
- эволюционный
- консервативный
- революционный
- пассивный

Тема 1.2. Основные законы и понятия современного информационного оборота

● 1. Режим защиты информации не устанавливается в отношении сведений, относящихся к:
+ деятельности государственных деятелей
- персональным данным
- государственной тайне

● 2. Не является объектом информационного правоотношения:
- недокументированная информация
- информационные продукты
- элементы информационной системы

● 3. Федеральный закон «О персональных данных» от 27 июля 2006 г. не регулирует отношения, возникающие при:
- обработке персональных данных, отнесенных к государственной тайне
- включении в Единый государственный реестр индивидуальных предпринимателей
- обработке персональных данных, отнесенных к служебной тайне

● 4. Один из основных объектов обеспечения информационной безопасности России:
- информационные продукты
- информационные ресурсы, содержащие сведения, которые относятся к государственной тайне и конфиденциальной информации
- квалифицированные кадры в области информационных технологий

● 5. Не является признаком информационного общества:
- мгновенная коммуникация членов общества друг с другом, вне зависимости от времени и от расстояния
- приоритетное развитие сельского хозяйства и промышленности на основе нанотехнологий
- общедоступность и постоянное обновление информационных данных

● 6. Исключите неправильный постулат:
- информация не существует без материального носителя
- содержание информации меняется одновременно со сменой материального носителя
- информация не связана с определенным конкретным носителем

● 7. В правовой режим документированной информации входит:
- тайна частной жизни
- банковская тайна
- электронная цифровая подпись

● 8. К служебной тайне не относится:
- профессиональная тайна
- вред, причиненный здоровью работника в связи с производственной травмой
- тайна деятельности соответствующего органа

● 9. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:
- об оплате труда работников некоммерческих организаций
- о системе оплаты и условиях труда
- которые составляют финансово-экономическую информацию и позволяют избежать неоправданных расходов

● 10. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:
- о безопасности пищевых продуктов
- об использовании новых технологий, позволяющих получить коммерческую выгоду
- об использовании безвозмездного труда граждан в деятельности некоммерческой организации

Тема 1.3. Современная криминологическая оценка преступлений в сфере компьютерной информации

● 1. Компьютерная преступность в узком смысле – ...
- совокупность преступлений, в которых компьютерная информация, компьютерные устройства, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи, защиты компьютерной информации являются не только предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления;
- совокупность преступлений, совершенных вменяемыми физическими лицами, посягающими на законные права и интересы государства, общества, физических и юридических лиц в сфере безопасного оборота (создания, хранения, обработки, передачи, получения, защиты и т.д.) компьютерной информации и функционирования компьютерных устройств, информационно-телекоммуникационных сетей и иных средств создания, использования, распространения компьютерной информации.
- (преступление с использованием компьютера) - любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных.

● 2. Заключенная в г. Будапеште 23 ноября 2001 года и ратифицированная почти 50-ю государствами Конвенция Совета Европы о преступности в сфере компьютерной информации закрепляет
- пять групп компьютерных преступлений;
- три группы компьютерных преступлений;
- четыре группы компьютерных преступлений;
- шесть групп компьютерных преступлений;

■ 3. Эксперты международной компании Group-IB, специализирующейся на предупреждении и расследовании киберпреступлений, считают, что основными преступными деяниями, образующими рынок киберпреступности в России, являются:
- продажа эксплойтов
- хищение электронных денег
- мошенничество в системах интернет-банкинга
- кибервымогательство
- хактивизм

■ 4. По мнению К. Н. Евдокимова, причинами компьютерной преступности являются:
- корыстные мотивы;
- несовершенство судебной практики;
- не достаточное финансирование правоохранительных органов;
- Российский менталитет.

■ 5. Путями преодоления латентности преступлений в сфере высоких технологий можно назвать
- повышение эффективности правоохранительной деятельности, требовательности к уровню профессионализма работников правоохранительных органов;
- использование экономико-правовых методов, основанных на анализе всех взаимосвязанных технико-экономических показателей деятельности хозяйственных субъектов;
- ужесточение уголовной ответственности;
- пересмотр динамического подхода к изучению компьютерной преступности.

● 6. Вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям
- фишинг
- спаминг
- крекинг
- хаккинг

● 7. К какому типу сетевых преступлений относится мошенничество (ст.159 УК РФ)?
- Нарушение нормального функционирования сетевой компьютерной системы.
- Несанкционированное проникновение в компьютерную систему, имеющую подключение к глобальной компьютерной сети.
- Несанкционированное внесение изменений в компьютерные данные (манипулирование данными).
- Публикация в глобальных компьютерных сетях материалов противоправного характера.

● 8. Среди сетевых преступлений какого типа наиболее распространенным является создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).
- Нарушение нормального функционирования сетевой компьютерной системы.
- Несанкционированное проникновение в компьютерную систему, имеющую подключение к глобальной компьютерной сети.
- Несанкционированное внесение изменений в компьютерные данные (манипулирование данными).
- Публикация в глобальных компьютерных сетях материалов противоправного характера.

■ 9. Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в:

- могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов
- серьёзное нарушение работы ЭВМ и их систем
- несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов
- замыкание электросети и электроприборов

■ 10. Преступления в сфере информационных технологий включают:
- распространение вредоносных вирусов
- неправильно выключить компьютер
- кражу номеров кредитных карточек
- украсть книжку из библиотеки
- взлом паролей
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет.

Раздел 2. «Правовые основы борьбы с компьютерной преступностью и компьютерными преступлениями»

Тема 2.1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ

● 1. Что такое компьютерная информация?
- это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.
- это информация, зафиксированная в периодических изданиях
- это серия и номер паспорта
- это персональные данные сотрудника госслужбы

● 2. Кем совершаются преступления в сфере компьютерной информации?
- ЭВМ
- компьютерной сетью Интернет
- человеком
- таких преступлений не существует

■ 3. По УК РФ преступлениями в сфере компьютерной информации являются:
- неправомерный доступ к компьютерной информации
- создание, использование и распространение вредоносных компьютерных программ
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
- кража компьютера из офиса
- неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

● 4. Сведения (сообщения, данные) независимо от формы их представления:
- информация
- информационные технологии
- информационная система
- информационно-телекоммуникационная сеть
- обладатель информации

● 5. Неквалифицированный состав неправомерного доступа к компьютерной информации является преступлением...
- средней тяжести
- тяжким
- с материальным составом
- особо тяжким

● 6. Что является объектом состава преступления, предусмотренного ст. 272 УК РФ ("Неправомерный доступ к компьютерной информации")?
- отношения в сфере обеспечения компьютерной безопасности
- отношения в сфере обеспечения безопасности работы с ЭВМ
- отношения в сфере охраны компьютерной информации
- отношения в сфере охраны компьютерных программ

● 7. Субъектом преступлений в сфере компьютерной информации является:
- физическое вменяемое лицо, достигшее 16-летнего возраста
- юридические и физические лица, не имеющие разрешения для работы с информацией определенной категории
- физическое вменяемое лицо, достигшее 18-летнего возраста
- физическое вменяемое лицо, достигшее 14-летнего возраста

● 8. Преступление, предусмотренное ст. 272 УК РФ, считается оконченным:
- с момента неправомерного доступа к охраняемой законом компьютерной информации
- только при наступлении определенных в законе общественно опасных последствий
- только при наступлении тяжких последствий
- с момента создания угрозы наступления определенных общественно опасных последствий

● 9. Часть 1 ст. 273 УК РФ является преступлением с ....
- формальным составом
- материальным составом
- усеченным составом
- квалифицированным составом

● 10. Субъективная сторона компьютерных преступлений характеризуется
- только умышленной виной в виде прямого умысла
- только неосторожной виной
- как умышленной, так и неосторожной виной
- только умышленной виной в виде прямого или косвенного умысла

Тема 2.2. Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации

● 1. Состав преступления в ст. 273 УК РФ сконструирован как:
- формальный
- безальтернативный
- материальный
- усеченный

● 2. Последовательное совершение действий указанных в диспозиции ст.273 УК РФ с одной и той же вредоносной программой либо иной компьютерной информацией ...
- образует идеальную совокупность преступлений
- образует реальную совокупность преступлений
- не образует совокупности преступлений

● 3. Состав преступления, предусмотренный ст. 272 УК РФ, по своей конструкции является
- материальным
- формальным
- усеченным

● 4. Модификация существующей компьютерной программы, охраняемой законом, и превращение ее во вредоносную ...
- подлежит квалификации по совокупности преступлений ст. 272 и ст.273 УК РФ
- не подлежит квалификации по совокупности преступлений, предусмотренных ст. 272 и ст. 273 УК РФ
- подлежит квалификации лишь только по ст. 272 УК РФ

- подлежит квалификации лишь только по ст. 273 УК РФ

● 5. Копирование программы без ее модификации ...
- не образует состава преступления, изложенного в ст. 272 УК РФ, так как не происходит неправомерного доступа к охраняемой законом компьютерной информации.
- образует состав преступления, предусмотренный ст.272 УК РФ если это деяние повлекло как модификацию, так и копирование компьютерной информации.
- образует состав преступления, предусмотренный ст.272 УК РФ если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

● 6. Копирование находящейся на материальном носителе информации, которая является объектом авторского права или смежных прав, при наличии законного доступа к ней, для использования или сбыта подлежит квалификации ...
- только по ст. 146 УК РФ при обязательном условии - деяние совершено в крупном размере.
- всегда только по ст. 146 УК РФ.
- по ст.272 УК РФ.
- по совокупности ст.146 и ст.272 УК РФ.

● 7. Пленум Верховного Суда Российской Федерации в постановлении от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» указал, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, ...
- требует дополнительной квалификации по ст.ст. 272, 273 или ст. 274.1 УК РФ.
- не требует дополнительной квалификации по ст.ст. 272, 273 или ст. 274.1 УК РФ.
- требует дополнительной квалификации по ст. 272 УК РФ.
- требует дополнительной квалификации по ст. 273 УК РФ.

● 8. Какая статья подлежит применению в случае когда виновный собирает, разглашает или использует сведения, составляющие коммерческую, налоговую или банковскую тайну, любым незаконным способом.
- ст. 183 УК РФ.
- ст. 272 УК РФ.
- ст.ст. 183 и 272 УК РФ.

● 9. Преступление, предусмотренное ст. 272 УК РФ, считается оконченным:
- с момента неправомерного доступа к охраняемой законом компьютерной информации;
- только при наступлении определенных в законе общественно опасных последствий;
- только при наступлении тяжких последствий;
- с момента создания угрозы наступления определенных общественно опасных последствий.

● 10. Преступление, предусмотренное ст. 273 УК РФ, признается оконченным с момента
- создания, распространения или использования вредоносных компьютерной программы или иной компьютерной информации независимо от наступления или ненаступления каких-либо последствий.
- наступления вредных последствий.
- создания угрозы наступления вредных последствий.

Тема 2.3. Вопросы квалификации преступлений в сфере компьютерной информации
● 1.: Какие преступления относятся к преступлениям в сфере компьютерной информации?
- создание вредоносных компьютерных программ
- распространение порнографических материалов с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»
- проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»
- все ответы правильные

■ 2. В виде информационных систем не могут выступать …
- депозитарии, банки, базы данных
- архивы, библиотеки
- Интернет-пользователи
- информационные продукты
- пресс-службы, институты

● 3. Субъектом преступлений в сфере компьютерной информации является:
- юридическое или физическое лицо, не имеющие разрешения для работы с информацией определенной категории
- физическое, вменяемое лицо, достигшее 18-летнего возраста
- физическое, вменяемое лицо, достигшее 16-летнего возраста
- физическое лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям

● 4. К компьютерной информации относятся:
- собственно информационные ресурсы (базы данных, текстовые, графические файлы и т.д.), представленные в форме электрических сигналов
- программы, обеспечивающие функционирование компьютера или информационно-телекоммуникационных сетей, хранение, обработку и передачу данных
- информация на машинном носителе, в компьютере или информационно-телекоммуникационных сетях
- все ответы правильные

● 5. Преступление, предусмотренное ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» считается оконченным:
- с момента совершения неправомерного доступа к охраняемой законом компьютерной информации.
- только в случае уничтожения, блокирования, модификации либо копирования компьютерной информации.
- только при наступлении тяжких последствий в случае уничтожения, блокирования, модификации либо копирования компьютерной информации.
- все ответы правильные.

● 6. В ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» не предусмотрена уголовная ответственность за:
- внесение изменений в существующие программы.
- распространение машинных носителей с вредоносными программами.
- несанкционированное копирование охраняемой законом компьютерной информации.
- нет правильного ответа.

● 7. Преступление, предусмотренное ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», считается оконченным:
- только при наступлении тяжких последствий.
- только в случае несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации.
- с момента использования или распространения вредоносной программы.
- с момента создания, использования или распространения вредоносной программы.

● 8. Субъектом преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», является:
- физическое, вменяемое лицо, достигшее 16-летнего возраста.
- физическое, вменяемое лицо, достигшее 18-летнего возраста.
- лицо, имеющее право на доступ к компьютеру или информационно-телекоммуникационным сетям.
- лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

● 9. В числе квалифицирующих признаков в ст. 273 УК РФ предусмотрено совершение данного преступления:
- с целью скрыть другое преступление или облегчить его совершение.
- из корыстной заинтересованности.
- из хулиганских побуждений.
- по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы.

■ 10. Преступление, предусмотренное ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», считается оконченным:
- с момента нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
- с момента уничтожения, блокирования, модификации либо копирования компьютерной информации.
- если это деяние причинило крупный ущерб.
- только при наступлении тяжких последствий.

Тема 2.4. Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации

● 1. На какой сессии Генеральной Ассамблеи ООН в 1946 г. была принята Резолюция 59 (I) под названием «Созыв международной конференции по вопросу о свободе информации»?
- второй
- первой
- третей
- пятой

● 2. По результатам работы какой сессии ГА ООН в 2000 году был одобрен новый проект резолюции, в котором отмечается, что для уменьшения и ограничения угроз в сфере информационной безопасности необходимо изучение международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем?
- 55-й сессии
- 54-й сессии
- 56-й сессии
- 57-й сессии

● 3. Право на свободу получения информации, обеспеченное международным правом, рассматривается как ...
- ограниченное
- абсолютное
- безусловное

■ 4. К угрозам международной информационной безопасности в соответствии с рекомендациями резолюции 55/28 не отнесены следующие факторы
- разработка и использование средств санкционированного вмешательства в работу информационных компьютерных систем;
- неправомерное использование и нанесение ущерба информационным ресурсам другого государства;
- целенаправленное информационное воздействие на критические инфраструктуры и население другого государства;
- действия, направленные на доминирование в информационном пространстве, поощрение терроризма и ведения информационных войн;
- поиск, получение и распространение информации и идей любыми средствами, и независимо от государственных границ.

● 5. Какая Конвенция не только рекомендует государствам-участникам закрепить на уровне национального законодательства важнейшие составы компьютерных преступлений, но и предписывает предпринимать конкретные организационные меры по борьбе с ними?
- Конвенция о борьбе с преступлениями в области информационных технологий Лиги арабских государств от 21 декабря 2010 г.
- Конвенция ООН «Об обеспечении международной информационной безопасности» 2012 г.
- Конвенция Совета Европы о киберпреступности от 2001г.

● 6. Конвенция Совета Европы о киберпреступности от 2001г. не ратифицирована
- США
- Россией
- Францией
- ОАЭ

● 7. Какое государство одним из первых приняло меры по установлению уголовной ответственности за совершение преступлений в сфере компьютерной информации?
- США
- Германия
- Великобритания
- Россия
- ОАЭ

● 8. В уголовном кодексе какой страны не существует специального раздела, посвященного компьютерным преступлениям?
- США
- Германия
- Голландия
- Россия
- Польша

● 9. Группа государств в законодательстве которых закреплен самостоятельный состав несанкционированного доступа.
- Австралия, Австрия, Бельгия, Дания, Франция
- Польша, Голландия, ФРГ, Турция
- Корея, Испания, Норвегия, Швеция, Швейцария

● 10. Группа государств в законодательстве которых несанкционированный доступ выступает в качестве способа совершения других преступлений.
- Корея, Испания, Норвегия, Швеция, Швейцария
- Австралия, Австрия, Бельгия, Дания, Франция
- Польша, Голландия, ФРГ, Турция

Тема 2.5. Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника

● 1. Отличительной особенностью причинности в криминальной сфере является
- информационный характер
- однозначность зависимостей
- процессуальная доказанность
- то, что причинность должна быть установлена в ходе следственного эксперимента

● 2. Условия преступности подразделяются на такие три основные группы, как
- по длительности действий, по содержанию, по источнику возникновения
- по времени действий, по природе возникновения, по уровню функционирования
- временная связь, связь состояний, статистическая связь
- сопутствующие, необходимые, достаточные

● 3. По источникам причины и условия компьютерной преступности различаются на

- криминогенные факторы и условия
- общие, отдельных видов преступлений и их конкретные проявления
- внутренние и внешние детерминанты
- объективные, объективно-субъективные, субъективные

● 4. В массиве латентной преступности выделяют
- четыре части
- пять частей
- три части
- две части

● 5. Коэффициент преступности — это
- цифра, характеризующая соотношение числа зарегистрированных преступлений с количеством населения
- цифра, характеризующая соотношение мужчин и женщин, совершивших преступления
- общее число лиц, совершивших преступления
- цифра, на которую увеличилось или уменьшилось число преступлений за год

● 6. Личность преступника — это
- его способы совершения преступлений
- его темперамент и его привычки
- совокупность криминогенных качеств, которые могут обусловить совершение какого-либо преступления
- его психопатологические особенности

● 7. Ведущая роль в формировании преступного поведения
- не зависит от личности вообще
- зависит только от ситуации
- зависит иногда от личности, иногда от ситуации
- зависит только от личности

■ 8. Из перечисленных пунктов, при изучении мотивации поведения, главным образом, исследуют
- наличие специальности
- семейное положение
- жизненные планы
- потребности личности
- социальные связи

● 9. Возраст относится к таким признакам структуры личности преступника, как
- уголовно-правовым
- социально-демографические
- нравственные свойства и психологические особенности
- социальной роли и социального статуса

● 10. К неблагоприятным тенденциям развития профессиональной преступности в России относят
- возрождение опасных криминальных профессий
- снижение образования и интеллектуального уровня преступников-профессионалов
- использование некриминальных навыков и знаний в криминальных целях, негативные социальные проявления
- появление такого негативного феномена, как преступный мир

Тема 2.6. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ

● 1. Какую ответственность влечет нарушение закона "Об информации, информационных технологиях и о защите информации"?
- дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством РФ

- гражданскую ответственность
- нет никакого наказания

● 2. Какие меры обеспечивают защиту информации?
- правовые, организационные и технические меры
- предотвращение несанкционированного доступа к информации
- постоянный контроль за обеспечением уровня защищенности информации

● 3. Выберите обязанности обладателя информации при осуществлении своих прав
- разрешать или ограничивать доступ к информации
- принимать меры по защите информации
- использовать информацию, в том числе распространять ее, по своему усмотрению
- передавать информацию другим лицам по договору или на ином установленном законом основании
- защищать установленными законом способами свои права

● 4. Меры информационной безопасности направлены на защиту от:
- нанесения неприемлемого ущерба
- нанесения любого ущерба
- подглядывания в замочную скважину

● 5. Что такое защита информации?
- защита от несанкционированного доступа к информации
- выпуск бронированных коробочек для дискет
- комплекс мероприятий, направленных на обеспечение информационной безопасности

● 6. Что понимается под информационной безопасностью?
- защита душевного здоровья телезрителей
- защита от нанесения неприемлемого ущерба субъектам информационных отношений
- обеспечение информационной независимости России

● 7. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
- доступность
- целостность
- конфиденциальность
- правдивое отражение действительности

● 8. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
- доступность
- масштабируемость
- целостность

● 9. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
- доступность
- целостность
- конфиденциальность

● 10. Что из перечисленного относится к числу основных аспектов информационной безопасности:
- возможность за приемлемое время получить требуемую информационную услугу
- невозможность отказаться от совершенных действий
- защита от несанкционированного доступа к информации

Инструкция по выполнению

В процессе решения тестов студент должен выбрать один или несколько верных ответов из предложенных вариантов ответов. На решение одного теста дается 2 минуты.

Критерии оценивания:
Максимальный балл – 10 баллов

8-10 баллов	Выставляется, если обучающийся ответил правильно на 84-100% заданий теста
5-7 баллов	Выставляется, если обучающийся ответил правильно на 67-83% заданий
2-4 баллов	Выставляется, если обучающийся ответил правильно на 50-66% заданий
0-1 баллов	Выставляется, если обучающийся ответил правильно на 0-49% заданий

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.

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию промежуточной аттестации. На зачете преподаватель может задать обучающемуся дополнительные вопросы. Зачет проводится преподавателем при наличии ведомости и зачетной книжки обучающегося. В ведомости и зачётной книжке обучающегося проставляются результаты промежуточной аттестации каждого обучающегося. В случае неявки обучающегося на промежуточную аттестацию в ведомости делается запись «не явился», допускается сокращение записи.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- лекции;
- практические занятия.

В ходе лекционных и практических занятий рассматриваются наиболее важные, существенные, сложные вопросы, которые трудно усваиваются студентами при изучении дисциплины. Углубляются и закрепляются приобретенные ими знания, развиваются навыки применения правовых норм для решения поставленных задач.

При подготовке к практическим занятиям каждый студент должен:
– освоить рекомендованную учебную литературу;
– при необходимости изучить статистические данные и судебную практику;
– подготовить ответы на все поставленные вопросы;

По согласованию с преподавателем обучаемый может подготовить одно эссе по предложенным им темам. В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Внеаудиторная самостоятельная работа студентов над курсом организована в форме: самостоятельной (домашней) работы, логически продолжающей аудиторные занятия по заданию преподавателя с установленными сроками исполнения. Дидактические цели: закрепление, углубление, расширение и систематизация знаний; формирование умений; самостоятельное овладение новым программным материалом; развитие самостоятельности мышления. Предусмотрены самостоятельные работы текущего и опережающего характера; самоконтроль.

Этапы выполнения заданий самостоятельной работы:
– определение целей самостоятельной работы;
– конкретизация поставленной задачи;
– самооценка готовности к самостоятельной работе по решению поставленной или выбранной задачи;
– выбор путей и средств для решения поставленной задачи;
– планирование (самостоятельно или с помощью преподавателя) самостоятельной работы по решению задачи;
– реализация программы выполнения самостоятельной работы;
– самоконтроль промежуточных и конечного результатов работы, их корректировка;
– определение причин и устранение выявленных ошибок.

Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, законспектировать прочитанный материал. Выделить непонятные термины, найти их значение в энциклопедических словарях.

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.

1. Методические рекомендации по изучению дисциплины в процессе аудиторных занятий

Изучение дисциплины требует систематического и последовательного накопления знаний.

Студентам необходимо вести конспект прочитанного материала. Перед очередным занятием необходимо просмотреть по конспекту предыдущий материал. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то следует обратиться к преподавателю (по графику его консультаций) или к преподавателю на практических занятиях.

Студентам следует:
- ознакомиться с заданием к занятию; определить примерный объем работы по подготовке к ним; выделить вопросы и задачи, ответы на которые или выполнение и решение без предварительной подготовки не представляется возможным;
- приносить с собой рекомендованную преподавателем литературу (её конспект) к конкретному занятию;
- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;
- пользоваться техническими средствами обучения и дидактическими материалами, которыми располагает учебное заведение.
- при подготовке к практическим занятиям следует обязательно использовать не только конспекты, учебную литературу, но и нормативно-правовые акты и материалы правоприменительной практики;

- теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;
- при ответах на вопросы и решения задач необходимо внимательно прочитать их текст и попытаться дать аргументированное объяснение с обязательной ссылкой на соответствующую правовую норму;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- по ходу практического занятия давать конкретные, четкие ответы по существу вопросов. Структура ответов может быть различной: либо вначале делается вывод, а затем приводятся аргументы, либо дается развернутая аргументация принятого решения, на основании которой предлагается ответ. Возможны и несколько вариантов ответов, которые должны быть обоснованны.
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенного анализа проблемной ситуации, в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

2. Методические рекомендации по выполнению различных форм самостоятельных заданий

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Студентам следует:
- руководствоваться графиком самостоятельной работы, определенным рабочей программой дисциплины;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на практических занятиях и консультациях неясные вопросы;
- использовать при подготовке нормативные документы университета, а именно, положение о написании письменных работ.

2.1. Методические рекомендации по работе с литературой.

Любая форма самостоятельной работы студента (подготовка к практическому занятию, написание эссе, курсовой работы, доклада и т.п.) начинается с изучения соответствующей литературы.

К каждой теме учебной дисциплины подобрана основная и дополнительная литература, которая указана в соответствующем разделе рабочей программы.

Основная литература - это учебники и учебные пособия.

Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, Интернет ресурсы.

Рекомендации студенту:

выбранную монографию или статью целесообразно внимательно просмотреть. В книгах следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро;
- в книге или журнале, принадлежащие самому студенту, ключевые позиции можно выделять маркером или делать пометки на полях. При работе с Интернет -источником целесообразно также выделять важную информацию;
- если книга или журнал не являются собственностью студента, то целесообразно записывать номера страниц, которые привлекли внимание. Позже следует возвратиться к ним, перечитать или переписать нужную информацию. Физическое действие по записыванию помогает прочно заложить данную информацию в «банк памяти».

Выделяются следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов. Хороший конспект должен сочетать полноту изложения с краткостью.

Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.

Тезисы - концентрированное изложение основных положений прочитанного материала.

Аннотация - очень краткое изложение содержания прочитанной работы. Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги.

Записи в той или иной форме не только способствуют пониманию и усвоению изучаемого материала, но и помогают вырабатывать навыки ясного изложения в письменной форме тех или иных теоретических вопросов.

2.2. Методические указания по написанию эссе.

Требования, предъявляемые к эссе:

1. Объем эссе не должен превышать 5-8 страниц. Печать производится через 1,5 интервала, размер шрифта 14 , с выравниванием по ширине. Левое поле листа 30 мм, правое – 10 мм, верхнее – 20 мм, нижнее 20 мм. Текст оформляется абзацами с отступом 1,25 см.
2. Эссе должно восприниматься как единое целое, идея должна быть ясной и понятной.
3. Необходимо писать коротко и ясно. Эссе не должно содержать ничего лишнего, должно включать только ту информацию, которая необходима для раскрытия авторской позиции, идеи.
4. Эссе должно иметь грамотное композиционное построение, быть логичным, четким по структуре.
5. Каждый абзац эссе должен содержать только одну основную мысль.
6. Эссе должно показывать, что его автор знает и осмысленно использует теоретические понятия, термины, обобщения, мировоззренческие идеи.
7. Эссе должно содержать убедительную аргументацию заявленной по проблеме позиции.

Структура эссе.

Эссе состоит из введения, основной части и заключения.

Во введении выделяют главную проблему, которую нужно раскрыть, и решить, каким образом эта проблема будет проанализирована.

В основной части целесообразно выстраивать систему аргументации на основе глубокой проработки темы и доказательств, обосновывающих высказанные утверждения. Следует выдвигать новые идеи по одной, в логической последовательности, которая даст возможность читателю проследить направление рассуждений. Эссе считается малой формой письменных работ, поэтому не принято делить основную часть на отдельные главы. Вместе с тем для удобства изложения и ясности логики аргументации основное содержание подразделяется на абзацы.

В заключении дается обобщение выдвинутых идей и освещаются ключевые моменты главной части работы. Как правило, заключение составляется в соответствии с названием работы. Также здесь можно указать направления дальнейшего исследования и изучения проблемы.