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

УТВЕРЖДАЮ
Директор Института магистратуры
Иванова Е.А.
«01» июня 2023г.

Рабочая программа дисциплины
Преступления в сфере цифровой информации

Направление 40.04.01 Юриспруденция
магистерская программа 40.04.01.01 "Цифровое право. Юрист в сфере информационных технологий"

Для набора 2023 года

Квалификация
магистр

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

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	7			
Вид занятий	УП	РП	УП	РП
Лекции	8	8	8	8
Практические	14	14	14	14
Итого ауд.	22	22	22	22
Контактная работа	22	22	22	22
Сам. работа	46	46	46	46
Часы на контроль	4	4	4	4
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 28.03.2023 протокол № 9.

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

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

Методическим советом направления: д.соц.н., к.ю.н., доцент, Федоренко Н.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	- комплексное изучение феномена преступлений в сфере обращения цифровой информации.
1.2	- формирование у студентов навыков юридического сопровождения процессов, связанных с обеспечением информационной безопасности и противодействия преступлениям, совершаемым в сфере обращения цифровой информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-3:Готов к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства
ПК-6:Способен осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению

В результате освоения дисциплины обучающийся должен:
Знать:
- социальную и правовую сущность юридического предписания; особенности отраслевой правосубъектности, виды участников правоотношений и их правовой статус, специфику выполнения должностных обязанностей в сфере профессиональной деятельности в целях обеспечения законности и правопорядка (соотнесено с индикатором ПК-3.1); - особенности и виды юридической ответственности в сфере осуществления профессиональной деятельности; систему мер общего, специального, индивидуального предупреждения правонарушений (соотнесено с индикатором ПК-6.1).
Уметь:
- анализировать правовые предписания и особенности их реализации, определять и разграничивать компетенцию органов публичной власти в сфере профессиональной деятельности (соотнесено с индикатором ПК-3.2); - выявлять противоправное поведение участников правоотношений, квалифицировать правонарушения и иные противоправные деяния в сфере осуществления профессиональной деятельности (соотнесено с индикатором ПК-6.2).
Владеть:
- действовать в соответствии с правовыми предписаниями в сфере профессиональной деятельности в целях обеспечения законности и правопорядка (соотнесено с индикатором ПК-3.3); - пресечения противоправной деятельности; устранения причин и условий, способствовавших совершению правонарушений, в том числе с помощью процессуальных средств, предусмотренных действующим законодательством (соотнесено с индикатором ПК-6.3).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Раздел 1. «Общая характеристика компьютерного оборота и уголовно-правовая природа преступлений в сфере обращения цифровой информации»				
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/	4	2	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
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. 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/	4	2	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2

1.3	Тема 1.3. Уголовно-правовая природа преступлений в сфере обращения цифровой информации 1. Понятие цифровой информации. 2. Понятие преступлений в сфере обращения цифровой информации. 3. Феномен безопасной компьютерной атаки. /Пр/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
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. /Ср/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
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. /Ср/	4	8	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
1.6	Тема 1.3. Уголовно-правовая природа преступлений в сфере обращения цифровой информации 1. Понятие цифровой информации. 2. Понятие преступлений в сфере обращения цифровой информации. 3. Феномен безопасной компьютерной атаки. /Ср/	4	8	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 2. Раздел 2. «Правовые основы борьбы с преступлениями в сфере обращения цифровой информации»				
2.1	Тема 2.1. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации 1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). 2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). 4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). 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). /Лек/	4	2	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2

2.2	Тема 2.2. Иные виды преступлений в сфере обращения цифровой информации 1. Мошенничество в сфере компьютерной информации. 2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов. 4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. 5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. /Лек/	4	2	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
2.3	Тема 2.1. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации 1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). 2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). 4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). 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/	4	6	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
2.4	Тема 2.2. Иные виды преступлений в сфере обращения цифровой информации 1. Мошенничество в сфере компьютерной информации. 2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов. 4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. 5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. /Пр/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2

2.5	Тема 2.1. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации 1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). 2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). 4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). 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). /Ср/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
2.6	Тема 2.2. Иные виды преступлений в сфере обращения цифровой информации 1. Мошенничество в сфере компьютерной информации. 2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов. 4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. 5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. /Ср/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
2.7	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. /Ср/	4	6	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2

2.8	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. /Ср/	4	8	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
2.9	Тема 2.5. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ 1. Основные направления профилактики преступлений в сфере компьютерной информации. 2. Конституционно-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. /Ср/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2
2.10	/Зачёт/	4	4	ПК-3 ПК-6	Л1.1 Л1.2Л2.1 Л2.2

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, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Заика А.	Компьютерная безопасность	Москва: Издательство «Рипол-Классик», 2013	http://biblioclub.ru/index.php?page=book&id=227317 неограниченный доступ для зарегистрированных пользователей
Л1.2	Мазуров В. А.	Компьютерные преступления: классификация и способы противодействия: Учебно-практическое пособие	Москва: Палеотип, 2002	http://www.iprbookshop.ru/48675.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	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

	Авторы, составители	Заглавие	Издательство, год	Колич-во
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

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

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 (МОДУЛЯ)

Помещения для проведения 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 (МОДУЛЯ)

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
ПК-3: Готов к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства			
Знать: - социальную и правовую сущность юридического предписания; особенности отраслевой правосубъектности, виды участников правоотношений и их правовой статус, специфику выполнения должностных обязанностей в сфере профессиональной деятельности в целях обеспечения законности и правопорядка;	- 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 по вопросам курса 1-36; Т–тест (темы 1-8); вопросы к зачету 1-25.
Уметь: - анализировать правовые предписания и особенности их реализации, определять и разграничивать компетенцию органов публичной власти в сфере профессиональной деятельности;	- 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 действовать в соответствии с правовыми	- выполняет кейс-задание с аргументацией	- студент правильно	КЗ – кейс-задание (темы 1-8); практико-ориентированные

предписаниями в сфере профессиональной деятельности в целях обеспечения законности и правопорядка.	полученного результата; - успешно выполняет практико-ориентированные задания для самостоятельной работы.	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).	задания (1-15).
ПК-6: Способен осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению			
Знать: – особенности и виды юридической ответственности в сфере осуществления профессиональной деятельности; систему мер общего, специального, индивидуального предупреждения правонарушений;	- 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).	ЭС – эссе (темы 1-30); практико-ориентированные задания (1-15).
Уметь: – выявлять противоправное поведение участников правоотношений, квалифицировать правонарушения и иные противоправные деяния в сфере осуществления профессиональной деятельности;	- 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-ориентированн	ЭС – эссе (темы 1-30); практико-ориентированные задания (1-15).

Владеть: - навыками пресечения противоправной деятельности; устранения причин и условий, способствовавших совершению правонарушений, в том числе с помощью процессуальных средств, предусмотренных действующим законодательством.	- выполняет кейс-задание с аргументацией полученного результата; - успешно выполняет практико-ориентированные задания для самостоятельной работы.	ых заданий в соответствии с действующими нормативно-правовыми актами и реальной судебной практикой; - объем выполненных заданий для самостоятельной работы (в полном, не полном объеме). - 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-задание (темы 1-8); 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:
84-100 баллов – оценка «зачтено»;
67-83 баллов – оценка зачтено»;
50-66 баллов – оценка «зачтено»;
0-49 баллов – оценка «не зачтено».

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

Вопросы к зачету:
1. Развитие техники как прогресс и источник социальных проблем.
2. Состояние, уровень, структура, динамика преступлений в сфере компьютерной информации.
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. Понятие и система преступлений в сфере компьютерной информации.
11. Основной состав преступления в виде неправомерного доступа к компьютерной информации.
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.
15. «Материальность» состава и виды обязательных последствий (уничтожение, блокирование, модификация, копирование или нейтрализация средств защиты компьютерной информации).
16. Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ.
17. Характеристика квалифицирующих признаков данного состава.
18. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
19. Бланкетная основа уголовной ответственности за компьютерное преступление.
20. Понятие информационно-телекоммуникационных сетей.
21. Преступления, совершаемые с использованием компьютерных технологий.
22. Отграничение преступлений в сфере компьютерной информации от смежных составов преступлений.
23. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).
24. 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".
25. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).

Практико-ориентированные задания к зачету

Задача №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?

Решение:
В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ "нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей". Законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.
Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.
Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности.
Однако, вопрос об уголовной ответственности Шатурина зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Задача №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.

Решение:
Действия лица следует квалифицировать по ст. 272 УК РФ, ч. 3. "Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, — наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок".
Как отмечено в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации" (утв. Генпрокуратурой России), уничтожение информации — это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени.
В указанном случае, было уничтожение данных.
Объект - общественные отношения, обеспечивающие сохранность компьютерной информации.
Объективная сторона - действия, состоящие в неправомерном доступе к компьютерной информации при отсутствии доступа таких лиц к ней. Уничтожение информации.
Субъект — вменяемое физическое лицо, достигшие возраста 16 лет.
Субъективная сторона -прямой умысел.

Задача №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?

Решение:
1. Статья 272 УК РФ Неправомерный доступ к компьютерной информации.
2. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Задача №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?

Решение:
1. Статья 273 УК РФ Создание, использование и распространение вредоносных программ для ЭВМ.
2. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Задача №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?

Решение:
1. Да, действия П. являются противозаконными.
2. Гражданин П. нарушил охраняемые законом общественные отношения – ст. 272 УК РФ Неправомерный доступ к компьютерной информации.
3. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Задача №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.

Решение:
Действия С. следует квалифицировать по п. ч.2 ст. 272 УК РФ.
Данный состав преступления является материальным и предполагает обязательное наступление одного или нескольких указанных в законе последствий:
- уничтожение информации - приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние;
- блокирование информации - создание условий ее недоступности, невозможности ее надлежащего использования;
- модификация (переработка) информации - любые изменения компьютерной информации, в том числе внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе.

Задача №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.

Решение:
Действия К. следует квалифицировать по п. ч.1 ст. 272 УК РФ "Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации".
Где:
- неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.
Другими словами, неправомерный доступ к компьютерной информации - это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной

информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее);

- уничтожение информации - это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени;
- блокирование информации - результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;
- модификация информации - внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;
- копирование информации - создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме - от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

Задача №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.?

Решение:

1. Копирование информации - создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме - от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

2. Ш., Л., П., Щ. будут нести уголовную ответственность за кражу, собирание сведений, составляющих банковскую тайну незаконным способом, а также за неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование компьютерной информации из корыстной заинтересованности группой лиц по предварительному сговору.

Задача №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?

Решение:
Действия знакомого должны быть квалифицированы как тайное хищение по ст. 158 УК РФ. Способ хищения — банковская карта.

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

Решение:
Действия квалифицируются по ч. 3 ст. 274.1 УК РФ. Ответственность за деяния, в зависимости от обстоятельств преступления и личности подсудимого, может быть назначена от принудительных работ на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Задача №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.

Решение:
Так как к ответственности привлекается специальный субъект — лицо, которое имеет законный доступ к ЭВМ и информационной системе, а негативные последствия наступили в результате невыполнения инструкций по безопасности и халатного отношения к обязанностям, то действия необходимо было квалифицировать по ч.1 ст. 274 УК РФ "Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб".

Задача №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?

Решение:
Студент К. виновен в совершении преступления по ч. 1, 2 ст. 273 (создание, использование и распространение вредоносных компьютерных программ), ч. 1 ст. 163 УК РФ (вымогательство).

Задача №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?

Решение:
Солдатова совершила преступление предусмотренное ч.2 ст.159.6 УК РФ "Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей совершенное с причинением значительного ущерба гражданину".

Задача №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?

Решение:
Сотрудник организации по халатности допустил вредные последствия для потерпевшего. Умысла прямого в действиях нет, программист не хотел повредить программное обеспечение школы. Однако он должен был предвидеть последствия, когда принес домой копию вредоносной программы и оставил в открытом доступе. Если образовательному учреждению причинен ущерб свыше 1 миллиона рублей, уничтожена или изменена информация, виновному грозит ответственность по ст. 274 УК РФ.

Задача №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?

Решение:
Согласно методическим рекомендациям Генеральной прокуратуры РФ "по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации", копирование информации - создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме - от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п. Следовательно, ознакомление с детализацией звонков невесты Ивановым следует считать копированием информации, подпадающим под действие ч.1 ст. 272 УК РФ "Неправомерный доступ к компьютерной информации".

Критерии оценки:
- 84-100 баллов (оценка «зачтено») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой; практико-ориентированное задание 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.

- 67-83 баллов (оценка «зачтено») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины; практико-ориентированное задание решено, 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.
- 50-66 баллов (оценка «зачтено») - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике; практико-ориентированное задание 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.
- 0-49 баллов (оценка «незачтено») - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы»; практико-ориентированное задание 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.

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. Уголовно-правовая природа преступлений в сфере обращения цифровой информации
1. Понятие цифровой информации.
2. Понятие преступлений в сфере обращения цифровой информации.
3. Феномен безопасной компьютерной атаки.

Раздел 2. «Правовые основы борьбы с компьютерной преступностью и компьютерными преступлениями»
Тема 2.1. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации
1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).
4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).
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).

Тема 2.2. Иные виды преступлений в сфере обращения цифровой информации
1. Мошенничество в сфере компьютерной информации.

2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.
3. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.
4. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.
5. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

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.

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. 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 оценки:
30 бальная оценка: ответы по каждой теме оцениваются максимум в 3 балла.
3 - 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 - 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 – 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 - имеются отдельные представления об изученном материале, но все же большая часть материала не усвоена, при ответе на вопросы допускает грубые ошибки.

Кейс- задание

Раздел 1. «Общая характеристика компьютерного оборота и компьютерной преступности»
Тема 1.1. Научно-технический прогресс и его последствия (побочные эффекты).
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 1.1.

Задача № 2
Составьте глоссарий к теме 1.1.

Задача № 3
Составьте 10 ситуационных задач по теме 1.1 и приведите их решение.

Тема 1.2. Основные законы и понятия современного информационного оборота.
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 1.2.

Задача № 2
Составьте глоссарий к теме 1.2.

Задача № 3
Составьте 10 ситуационных задач по теме 1.2 и приведите их решение.

Тема 1.3. Уголовно-правовая природа преступлений в сфере обращения цифровой информации
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 1.3.

Задача № 2
Составьте глоссарий к теме 1.3.

Задача № 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. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 2.1.

Задача № 2
Составьте глоссарий к теме 2.1.

Задача № 3
Составьте 10 ситуационных задач по теме 2.1 и приведите их решение.

Тема 2.2. Иные виды преступлений в сфере обращения цифровой информации
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 2.2.

Задача № 2
Составьте глоссарий к теме 2.2.

Задача № 3
Составьте 10 ситуационных задач по теме 2.2 и приведите их решение.

Тема 2.3. Вопросы квалификации преступлений в сфере компьютерной информации
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 2.3.

Задача № 2
Составьте глоссарий к теме 2.3.

Задача № 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.
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 2.4.

Задача № 2
Составьте глоссарий к теме 2.4.

Задача № 3
Составьте 10 ситуационных задач по теме 2.4 и приведите их решение.

Тема 2.5. Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.
Задача № 1
Подберите и перечислите источники информации, имеющие отношение к теме 2.5.

Задача № 2
Составьте глоссарий к теме 2.5.

Задача № 3
Составьте 10 ситуационных задач по теме 2.5 и приведите их решение.

Критерии оценки:
30 бальная: каждая кейс-задача оценивается максимум в 3 балла.
3 - кейс-задача решена 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 - кейс-задача решена 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 - кейс-задача решена, 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 - кейс-задача решена 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 оценки:
Студент за семестр готовит одно эссе по предложенным темам. Максимальный балл – 30.
21-30 баллов – блестящая работа, которая отвечает всем предъявляемым требованиям, а также отличается научной новизной и является вкладом в развитие правовой науки.
16-20 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.
11-15 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.
6-10 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.

Тема 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 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 3. Уголовно-правовая природа преступлений в сфере обращения цифровой информации

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 4. Преступления в сфере компьютерной информации по уголовному кодексу российской федерации как виды преступлений в сфере обращения цифровой информации

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 5. Иные виды преступлений в сфере обращения цифровой 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 6. Вопросы квалификации преступлений в сфере компьютерной информации

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 7. 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 8. 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 оценки:
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:

- практические занятия.

В ходе 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 методом устного опроса или 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 семинара 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 семинарах 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 семинарскому 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 (Times New Roman), 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.