Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Артеменков Михаил Николаевич
Должность: Ректор
Дата подписания: 02.11.2026 17:51:14
Уникальный программный ключ:
a63b74166e8f4fc17bd1e0462725f79e393bfdf9

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра уголовно-правовых дисциплин

«Утверждаю»
Проректор по учебно-методической работе
_____Ю.А. Устименко
« 16 » июня 2022 г.

Рабочая программа дисциплины
Б1.О.12 Преступления в сфере высоких технологий

Направление подготовки: 40.04.01. «Юриспруденция»
Направленность (профиль): Уголовное право, уголовный процесс
Форма обучения – очная
Курс – 2
Семестр – 4
Всего зачетных единиц – 3, часов – 108
Форма отчетности: зачет – 4 семестр.

Программу разработал
Доктор юридических наук Лопатина Т.М.

Одобрена на заседании кафедры
«09» июня 2022 г., протокол № 10

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина «Преступления в сфере высоких технологий» относится к обязательной части учебного плана по направлению подготовки 40.04.01 «Юриспруденция», направленность (профиль): Уголовное право, уголовный процесс, изучается в пятом семестре.

В ходе изучения дисциплины студенты опираются на знания и умения, полученные при изучении таких дисциплин, как Актуальные проблемы уголовного права, Основы квалификации преступлений, Актуальные проблемы уголовно-процессуального права.
Изучение дисциплины необходимо для последующего успешного освоения таких дисциплин, как «Актуальные проблемы предупреждения современной преступности», а также прохождения преддипломной практики, выполнения научно-исследовательской работы и выпускной квалификационной работы.

2. Планируемые результаты обучения по дисциплине

Компетенция	Индикаторы достижения
Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований (ОПК-7)	**Знать:** методы и средства поиска, систематизации и обработки правовой информации в сфере профессиональной деятельности. **Уметь:** применять современные информационные технологии для поиска и обработки правовой информации, проведения статистического анализа информации в сфере профессиональной деятельности. **Владеть:** навыками работы в правовых информационных системах; навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.
Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности (ПК-1)	**Знать:** законодательство в сфере процессуального и материального права, необходимое для правоприменительной деятельности; основные методы и способы квалификации противоправных действий, совершаемых в области действия норм отраслевого законодательства; основные функции уполномоченных органов и должностных лиц с целью выявления и фиксирования действий и (или) бездействий, нарушающих права и законные интересы и причиняющих ущерб интересам государства, общества, физическим и юридическим лицам. **Уметь:** руководствоваться нормативными правовыми актами в конкретных сферах юридической деятельности при реализации норм материального и процессуального права; анализировать и оценивать факты и противоправные действия (бездействия), нарушающие права и законные интересы граждан и организаций и наносящие ущерб

	интересам государства, общества, физическим и юридическим лицам. **Владеть:** навыками и умениями квалифицированного применения нормативных правовых актов в конкретных сферах юридической деятельности; способностью применять соответствующие нормы материального и процессуального права с целью выявления и фиксации действий и (или) бездействий, причиняющих ущерб интересам государства, общества, физических и юридических лиц; навыками составления юридических документов в системе правоприменительной деятельности.

3. Содержание дисциплины

Преступления в сфере высоких технологий - новый вид преступных посягательств в уголовном законодательстве Российской Федерации. Экономические, социальные, техногенные факторы, обусловившие появление преступлений в сфере компьютерной информации. Сущность информационного общества. Общая характеристика процесса компьютеризации. Характеристика степени общественной опасности компьютерных преступлений. Мировой законодательный опыт борьбы с компьютерными преступлениями: Швеция, США, ФРГ. Межгосударственное сотрудничество в борьбе с компьютерной преступностью. Internet – глобальное информационное пространство и инструмент для совершения преступлений. Вопросы противодействия преступности в Internet.

Информационные отношения как объект уголовно-правовой охраны. Теоретическое понятие объекта преступного посягательства. Подходы к определению понятия объекта преступления. Соотношения объекта и предмета преступного посягательства. Понятие предмета компьютерного преступления. Обзор точек зрения. Понятие компьютерной информации. Понятие компьютерной программы. Информация как особый объект правового регулирования.

Понятие компьютерного преступления. Обзор точек зрения на понятие «компьютерная преступность». Виды преступлений в сфере компьютерной информации.

Виды и способы совершения преступлений в сфере высоких технологий. Проблема классификации и определения названий способов совершения преступлений в сфере высоких технологий. Многообразие способов совершения преступлений в сфере высоких технологий. Зарубежный опыт классификации способов совершения преступлений в сфере высоких технологий. Классификация способов совершения преступлений в сфере высоких технологий.

Своеобразие способов совершения компьютерных преступлений по уголовному законодательству стран СНГ и государств, образованных на постсоветском пространстве: Республика Беларусь, Республика Таджикистан, Узбекистан, Азербайджанская Республика, Латвийская Республика, Эстонская Республика.

Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации. Понятие неправомерного доступа к охраняемой законом компьютерной информации. Понятие собственника и владельца информационных ресурсов. Способы достижения неправомерного доступа к охраняемой законом компьютерной информации. Общая характеристика научных дискуссий по форме вины при неправомерном доступе к компьютерной информации. Форма вины. Вопросы уголовной ответственности за

совершение неправомерного доступа к охраняемой законом компьютерной информации по неосторожности. Квалифицированные виды состава преступления.

Вопросы уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ. Обязательные признаки объективной стороны. Понятие «вируса» и «вредоносной» компьютерной программы. Создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Способы распространения компьютерной информации. Использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Общая характеристика субъективной стороны состава. Квалифицированные виды состава преступления.

Уголовно-правовой анализ состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Характеристика бланкетности диспозиции уголовно-правовой нормы. Понятие правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информациии информационно-телекоммуникационных сетей. Понятие правил эксплуатации информационно-телекоммуникационных сетей и оконечного оборудования. Понятие правил доступа к информационно-телекоммуникационным сетям. Уголовно-наказуемое 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. Субъективная сторона преступления. Форма вины. Квалифицирующие деяние признаки: тяжкие последствия или угроза их наступления.

Типология личности компьютерного преступника. Понятие «личность преступника» в теории уголовного права. Основания типологии личности преступника. Законодательная классификация субъектов компьютерных преступлений. Криминологическая характеристика личности преступника. Личностные характеристики субъекта преступления в сфере высоких технологий.

Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий. Некоторые теоретические вопросы борьбы с преступлениями в сфере высоких технологий. Меры противодействия преступлениям в сфере высоких технологий: организационно-управленческие, технические и правовые.

Понятие и виды контроля над преступностью. Социальный, правовой контроль. Виды и содержание правового контроля над преступностью, связанной с использованием компьютерной информации. Позитивный правовой контроль. Репрессивный правовой контроль. Задачи и средства комплексного контроля над преступностью в сфере высоких технологий. Международный опыт борьбы с преступлениями в сфере высоких технологий. Опыт правового регулирования общественных отношений в сфере высоких технологий в Российской Федерации.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий				
			лекции	семинары	лаб. занятия	практич. занятия	сам. работа
1.	Преступления в сфере высоких технологий - новый вид преступных посягательств в уголовном законодательстве Российской Федерации	14	2			2	10
2	Информационные отношения как объект уголовно-правовой охраны	14	2			2	10
3	Виды и способы совершения преступлений в сфере высоких технологий	12	2				10
4	Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации	12				2	10
5	Вопросы уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ	12				2	10
6	Вопросы уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	12				2	10
7	Типология личности компьютерного преступника	16	2			2	12
8	Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий.	16	2			2	12
	Итого	**108**	**10**			**14**	**84**

5. Виды образовательной деятельности

Занятия лекционного типа

Тема 1. Преступления в сфере высоких технологий - новый вид преступных посягательств в уголовном законодательстве Российской Федерации

План

1. Сложность в квалификации деяний, совершенных в сфере компьютерной информации.
2. Соотношение состава неправомерного доступа к компьютерной информации и состава создания, использования и распространения вредоносных компьютерных программ по объективным и субъективным признакам.
3. Разграничение составов неправомерного доступа к компьютерной информации и нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (самостоятельная работа).
4. Соотношение со смежными составами (самостоятельная работа).

Тема 2. Информационные отношения как объект уголовно-правовой охраны

План

1.Информационные отношения как предмет правового регулирования. 2.Понятие информационной безопасности. Источники угроз информационной безопасности.

3.Структура информационной безопасности как объекта уголовно - правовой охраны.

4. Информация как объект информационных отношений предмет преступлений против информационной безопасности. Категории информации по критериям доступа к ней и распространения.

5. Законодательство РФ в области обеспечения информационной безопасности

Тема 3. Виды и способы совершения преступлений в сфере высоких технологий

План

1. Многообразие способов совершения преступлений в сфере высоких технологий.
2. Классификация способов совершения компьютерных преступлений по законодательству России.
3. Сложность в квалификации деяний, совершенных в сфере высоких технологий.
4. Перечень смежных составов, предусматривающих неправомерное обращение с информацией по уголовному кодексу Российской Федерации.
5. Проблема ответственности за компьютерное мошенничество.

Тема 7. Типология личности компьютерного преступника

План

1. Классификация субъектов компьютерных преступлений.
2. Основные характеристики личности преступника в сфере высоких технологий.
1. Варианты типологии личности компьютерных преступников по уровню профессиональной подготовки.
2. Варианты типологии личности компьютерных преступников по социальному положению.
3. Варианты типологии личности компьютерных преступников по противоправной направленности.
4. Варианты типологии личности компьютерных преступников по возможности доступа к средствам компьютерной техники.
5. Соотношение понятий: «компьютерный преступник», «хакер» и «крекер».

Тема 8. Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий.

План

1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах.
2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.
3. Сравнительно-правовой анализ преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.
4. Международные соглашения в сфере борьбы с компьютерными преступлениями (Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г.).
5. Международный и зарубежный опыт регулирования ответственности за преступления, совершаемые с использованием глобальных компьютерных сетей (сети Интернет).

Занятия семинарского типа (практические занятия)

Тема 1. Преступления в сфере высоких технологий - новый вид преступных посягательств в уголовном законодательстве Российской Федерации

Вопросы для обсуждения:

1. Понятие преступлений против информационной безопасности, их место в системе информационных преступлений. Понятие киберпреступности.
2. Система преступлений против информационной безопасности по российскому уголовному законодательству.
3. Преступления против информационной безопасности и преступления в сфере компьютерной информации: соотношение и взаимосвязь.

Тема 2. Информационные отношения как объект уголовно-правовой охраны

Вопросы для обсуждения:

1. Понятие родового объекта преступных посягательств в сфере высоких технологий.
2. Понятие предмета компьютерного преступления.
3. Понятие и виды преступлений в сфере высоких технологий.

Самостоятельная работа студентов – подготовка презентации по одному из вопросов, вынесенных на рассмотрение (по выбору магистранта) – 11 часов.

Литература.

Основная: 1-4.

Тема 4.Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации. Тема 5. Вопросы уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ.

Вопросы для обсуждения:

1. Характеристика объективных признаков составов преступлений.
2. Понятие охраняемой законом компьютерной информации (самостоятельная работа).
3. Понятие «вируса» и «вредоносной» компьютерной программы (самостоятельная работа).

4. Характеристика субъективных признаков составов преступлений.
5. Совершение неправомерного доступа к компьютерной информации по неосторожности (самостоятельная работа).
6. Особенности субъекта преступлений (самостоятельная работа).

Самостоятельная работа студентов – подготовка презентации по одному из вопросов, вынесенных на рассмотрение (по выбору магистранта) – 24 часа.

Литература.
Основная: 1-4.

Тема 6. Вопросы уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Вопросы для обсуждения:

1. Характеристика бланкетности диспозиции уголовно-правовой нормы.
2. Понятие правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информациии информационно-телекоммуникационных сетей.
3. Понятие правил эксплуатации и доступа к информационно-телекоммуникационным сетям.

Тема 7. Типология личности компьютерного преступника

Вопросы для обсуждения:

1. Особенности субъектов компьютерных преступлений.
2. Классификация субъектов компьютерных преступлений (самостоятельная работа).
3. Личностный аспект субъекта компьютерного преступления.
4. Основные характеристики личности компьютерного преступника (самостоятельная работа).

Самостоятельная работа студентов – подготовка презентации по одному из вопросов, вынесенных на рассмотрение (по выбору магистранта) – 11 часов.

Литература.
Основная: 1-4.

Тема 8. Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий

Вопросы для обсуждения:

1. Международное сотрудничество как форма борьбы с преступностью в сфере высоких технологий.
2. Понятие, задачи и средства комплексного контроля над преступностью в сфере высоких технологий.
3. Международный опыт борьбы с преступлениями в сфере высоких технологий.
4. Опыт правового регулирования общественных отношений в сфере высоких технологий в Российской Федерации.

Самостоятельная работа студентов – подготовка презентации по одному из вопросов, вынесенных на рассмотрение (по выбору магистранта) – 11 часов.

Литература.
Основная: 1-4.

Самостоятельная работа

Тема 1. Преступления в сфере высоких технологий- новый вид преступных посягательств в уголовном законодательстве Российской Федерации

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

1. Ретроспектива создания первых счетных машин и их модификация в современные компьютеры.
2. Международный опыт противодействия преступлениям в сфере высоких технологий.
3. Основные этапы межгосударственного сотрудничества в борьбе с преступностью в сфере высоких технологий.
4. Проблема создания эталонной схемы закона об уголовной ответственности за совершение компьютерных преступлений Organization for Economic Cooperation and Development.
5. Классификация компьютерных преступлений, предложенная экспертами ООН.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Основы компьютерного законодательства США».
2. Подготовить эссе на тему: «Internet – государство в государстве».
3. Подготовить эссе на тему: «Ответственность за компьютерные преступления по уголовному законодательству государств-участников СНГ».

Тема 2. Информационные отношения как объект уголовно-правовой охраны

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

1. Категория объекта в современной уголовно – правовой теории.
2. Понятие информации в различных аспектах.
3. Понятие компьютерного преступления и преступления в сфере высоких технологий.
4. Характеристика точек зрения на понятие «компьютерное преступление».
5. Компьютерное преступление как вид информационного преступления, посягающего на информационные отношения.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Понятие компьютерной информации».
2. Подготовить эссе на тему: «Виды преступлений в сфере высоких технологий».
3. Подготовить эссе на тему: «Особенности законодательной конструкции составов преступлений в сфере робототехники».

Задачи

1. Школьник 9 класса П. приобрел на рынке у неизвестного лица диск. П., имея опыт работы с компьютером и его программным обеспечением, заведомо зная, что на данном диске содержится информация в виде компьютерных программ, зараженных кодом программ-вирусов, которые при запуске приводят к уничтожению информации. П. принес данный диск к своему родственнику на работу и с разрешения последнего установил диск на его рабочем компьютере. При запуске программы вся служебная информация, содержащаяся в персональном компьютере родственника П., была уничтожена. В результате работа отдела, в котором работал родственник П., была парализована на несколько дней.

Влекут ли действия несовершеннолетнего П. уголовную ответственность?

Как квалифицировать действия родственника несовершеннолетнего П.?

2. 15-летний школьник С., чтобы доказать своим сверстникам уровень своей компьютерной подготовленности, преодолел систему защиты одного из частных коммерческих банков, о чем рассказал своим друзьям и в доказательство распространил

среди них информацию о способе взлома системы защиты банка. Один из его друзей К. воспользовался полученной информацией, взломал систему защиты банка и перечислил 100 тыс. рублей со счета банка на депозитный счет своего отца. В ходе следствия было установлено, что несовершеннолетний С., взламывая систему защиты банка, не преследовал корыстных целей.

Подлежит ли несовершеннолетний С. уголовной ответственности?

Как должен решаться вопрос об ответственности К.?

Тема 3. Виды и способы совершения преступлений в сфере высоких технологий

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

1. Основные классификации способов совершения преступлений в сфере высоких технологий.
2. Способы совершения компьютерных преступлений по уголовному законодательству некоторых государств-участников СНГ.
3. Своеобразие способов совершения компьютерных преступлений по уголовному законодательству Республики Беларусь.
4. Своеобразие способов совершения компьютерных преступлений по уголовному законодательству Республики Таджикистана.
5. Своеобразие способов совершения компьютерных преступлений по уголовному законодательству Узбекистана.
6. Своеобразие способов совершения компьютерных преступлений по уголовному законодательству Азербайджанской Республики.
7. Своеобразие способов совершения компьютерных преступлений по уголовному законодательству Латвийской Республики.
8. Своеобразие способов совершения компьютерных преступлений по уголовному законодательству Эстонской Республики.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Характеристика основных групп способов совершения преступлений в сфере высоких технологий».
2. Подготовить эссе на тему: «Зарубежный опыт классификации способов совершения преступлений в сфере высоких технологий».

Тема 4.Вопросы уголовной ответственности за неправомерный доступ к компьютерной информации

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

1. Понятие охраняемой законом компьютерной информации.
2. Совершение неправомерного доступа к компьютерной информации по неосторожности.
3. Особенности субъекта преступлений в сфере высоких технологий.
4. Сущность уголовно-правового запрета, установленного собственником на доступ к компьютерной информации.
5. Виды охраняемой законом информации.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Ответственность за несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины?».
2. Подготовить эссе на тему: «Внутренние пользователи: опасность изнутри компании».
3. Подготовить эссе на тему: «Преступные последствия неправомерного доступа к компьютерной информации».

4. Подготовить эссе на тему: «Специальный субъект неправомерного доступа к компьютерной информации».

Задачи

1. Работник коммерческой организации «Окна» В., не имеющий достаточного опыта работы на компьютере, случайно удалил из памяти главного компьютера организации информацию о её новых разработках, из-за чего эта организация понесла значительные убытки. По заявлению директора в отношении В. было возбуждено уголовное дело.

Подлежит ли уголовной ответственности В.?

2. Компьютерный энтузиаст Д., придерживаясь определенных политических взглядов, в разгар предвыборной кампании проник в один из «серверов имен» глобальной сети Internet и подменил сетевой адрес web – сайта партии «ЛДПР» на адрес webсайта КПРФ, из-за чего все пользователи сети, запрашивающие новости партии «ЛДПР», попадали на агитационную страницу КПРФ.

Как квалифицировать действия Д.?

Вариант: Д. являлся администратором данного «сервера имен» и в силу этого имел легальный доступ к соответствующей информации.

Можно ли при таких обстоятельствах привлечь Д. к уголовной ответственности?

Тема 5. Вопросы уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

1. Понятие «вируса» и «вредоносной» компьютерной программы, робота.
2. Понятие и способы распространения вредоносных компьютерных программ.
3. Классификация вирусов.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Создание компьютерной программы как процесс написания её алгоритма».

2. Подготовить эссе на тему: «Способы распространения вредоносных компьютерных программ».

3. Подготовить эссе на тему: «Понятие «вируса».

4. Подготовить эссе на тему: «Особенности формы вины при создании, использовании и распространении вредоносных компьютерных программ, повлекшие тяжкие последствия или создавших угрозу их наступления».

Задачи

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

Как квалифицировать действия И.?

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

Дайте правовую оценку действиям А.

3. Работник коммерческой организации «Салют» В., не имеющий достаточного опыта работы на компьютере, «заразил» компьютерную систему организации вирусом, записанном на его диске. В. не знал о наличии вируса, поскольку, следуя ранее изданному приказу руководства организации, проверил диск с помощью антивирусной программы, но данная программа была устаревшей и не могла идентифицировать новые виды вирусов, что было известно В.

Как в таком случае квалифицировать действия В.?

4. М. заключил договор с медицинской фирмой «Диабет», в соответствии с условиями которого, он обязался создать компьютерную программу для нужд фирмы, а та, в свою очередь, оплатить М. его работу. В процессе написания программы М. неоднократно, в целях согласования ее параметров, предоставлял работникам фирмы черновые варианты программы, записанные на диске. Через некоторое время руководитель фирмы К. заявил М., что в его дальнейших услугах фирма не нуждается, договор между ними расторгается, а оплата его работы произведена не будет, так как на это в настоящее время у фирмы нет денег. Опасаясь такого развития событий, М. еще заранее запрограммировал последний черновой вариант заказанной ему программы таким образом, чтобы программа потеряла свою функциональность спустя несколько дней после начала её использования.

Именно этот вариант К. распорядился установить в компьютерную сеть своей фирмы несмотря на то, что договором не предусматривалось право фирмы каким-либо образом использовать черновые варианты разрабатываемой М. программы. Следствием выхода программы из строя послужила дезорганизация деятельности фирмы, что повлекло ухудшение состояния здоровья нескольких десятков больных.

По заявлению К. в отношении М. было возбуждено уголовное дело, а действия М. были квалифицированы по ч. 3 ст. 273 УК РФ. Адвокатом М. были заявлены ходатайства об освобождении последнего от уголовной ответственности за отсутствием в его действиях состава преступления и о возбуждении в отношении К. уголовного дела по признакам ч. 2 ст. 272 УК РФ.

Какое решение должен принять следователь?

Содержатся ли в действиях К. признаки состава преступления?

Вариант: М. запрограммировал уничтожение данных в компьютерной системе фирмы как реакцию на нелегальное использование черновой копии его программы.

Изменится ли в данном случае юридическая оценка его действий?

5. Работник банка Р. скопировал принадлежащую банку компьютерную программу, которая препятствовала несанкционированному доступу к банковской информации. В дальнейшем он, через своих знакомых, продал указанную программу Б., который, в свою очередь, договорился с М. и С. присвоить себе 300 тыс. рублей из указанного банка, поручив анализ программы программисту У.

У. ради профессионального интереса, не зная об истинных намерениях вышеупомянутых лиц, проанализировал компьютерную программу, вскрыл её слабые места и передал результаты своей работы С. Б., будучи сам программистом, используя данные, полученные от У., сумел перевести 300 тыс. рублей со счета указанного банка на счет, открытый в ином банке на имя М., который и снял с этого счета всю переведенную сумму.

Квалифицируйте действия Б., С. и М.

Подлежат ли уголовной ответственности Р. и У.?

6. Студенты университета К. и Х. разработали и осуществили атаку «отказ в обслуживании» на поисковый сервер «Yandex» сети Internet, заключавшуюся в отправке огромного количества запросов на поиск в сети с нескольких компьютеров лаборатории университета. В результате этого доступ к серверу других пользователей сети Internet был полностью заблокирован на срок более 2 часов.

Будучи допрошенными по обстоятельствам дела К. и Х. пояснили, что они хотели «повалить сервер», руководствуясь исключительно желанием проверить свои способности к этому.

Решите вопрос об ответственности К. и Х.

Тема 6. Вопросы уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

6. Характеристика бланкетности диспозиции уголовно-правовой нормы.
7. Понятие правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информациии информационно-телекоммуникационных сетей.
8. Понятие правил эксплуатации и доступа к информационно-телекоммуникационным сетям.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Правила эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информациии информационно-телекоммуникационных сетей.
2. Подготовить эссе на тему: «Правила эксплуатации информационно-телекоммуникационных сетей и оконечного оборудования».
3. Подготовить эссе на тему: «Правила доступа к информационно-телекоммуникационным сетям».

Задачи

1. Главный врач санатория В., используя служебный компьютер в личных целях, загрузила его новыми программами. В результате чего из-за нехватки оперативной памяти другие медицинские программы были уничтожены. В результате уничтожения охраняемой законом компьютерной информации, санаторию был причинен существенный вред, выразившейся в утрате информации, необходимой для лечения пациентов и дезорганизации работы установки лазерной терапии.

Квалифицируйте действия главного врача В.

2. Работник коммерческой организации Т., в обязанность которого входило техническое обслуживание компьютерной системы фирмы, из-за недобросовестного отношения к своим служебным обязанностям не проводил профилактики компьютеров, в частности периодических проверок на антивирусный контроль. В результате чего сроки технического обслуживания компьютеров были нарушены, в операционном зале постоянно не выдерживался температурный режим. Все это привело к сбою в работе компьютерной системы фирмы, что послужило основанием к прекращению её деятельности на несколько дней, чем фирме был причинен крупный материальный вред.

Как квалифицировать действия Т.?

Тема 7. Типология личности компьютерного преступника.

Формы и виды контроля знаний студентов на занятиях

Вопросы для самостоятельного изучения:

3. Классификация субъектов компьютерных преступлений.
4. Основные характеристики личности преступника в сфере высоких технологий.
9. Варианты типологии личности компьютерных преступников по уровню профессиональной подготовки.
10. Варианты типологии личности компьютерных преступников по социальному положению.
11. Варианты типологии личности компьютерных преступников по противоправной направленности.
12. Варианты типологии личности компьютерных преступников по возможности доступа к средствам компьютерной техники.

13. Соотношение понятий: «компьютерный преступник», «хакер» и «крекер».

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Особенности субъектов компьютерных преступлений».
2. Подготовить эссе на тему: «Хакер: компьютерный преступник или рядовой пользователь компьютерной техники?».
3. Подготовить эссе на тему: «Личностный аспект субъекта компьютерного преступления».
4. Робот как субъект компьютерного преступления.

Тема 8. Мировой опыт правового регулирования предупреждения преступности в сфере высоких технологий

Вопросы для самостоятельного изучения:

1. Криминологическая характеристика состояния преступности в сфере высоких технологий.
2. Понятие и виды источников угроз информационной безопасности.
3. Национальная правовая база противодействия преступлениям в сфере высоких технологий.
4. Источники угроз информационной безопасности.
5. Опыт правового регулирования общественных отношений в сфере высоких технологий в Российской Федерации.

Задания для самостоятельной работы:

1. Подготовить эссе на тему: «Новейшие виды источников угроз информационной безопасности».
2. Подготовить эссе на тему: «Мировой опыт противодействию преступлениям высоких технологий».
3. Подготовить эссе на тему: «Правовое регулирование ответственности за мошенничество с использованием компьютерных технологий».
4. Подготовить эссе на тему:«Состояние преступности в сфере компьютерной информации в РФ».
5. Подготовить эссе на тему: «Качественная характеристика преступности высоких технологий в РФ».

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Устный опрос.

Критерии оценивания ответа на теоретический вопрос

Отлично	Студент обнаруживает систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой по вопросу, свободно оперирует приобретенными знаниями, применяет их в практических ситуациях
Хорошо	Студент демонстрирует прочные знания учебного материала, но допускает незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний на новые, нестандартные ситуации, усвоил основную литературу
Удовлетворительно	Студент демонстрирует базовые знания учебного материала, но допускает значительные ошибки, проявляет пробелы в знаниях по отдельным вопросам, испытывает значительные затруднения при оперировании знаниями и их применением в практических

	ситуациях.
Неудовлетворительно	Студент проявляет недостаточность знаний, не знаком с основной литературой по вопросу, не способен применять знания в практических ситуациях

Задача.

Примерный перечень задач.

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

Дайте правовую оценку действиям А.

2. Студенты университета К. и Х. разработали и осуществили атаку «отказ в обслуживании» на поисковый сервер «Yandex» сети Internet, заключавшуюся в отправке огромного количества запросов на поиск в сети с нескольких компьютеров лаборатории университета. В результате этого доступ к серверу других пользователей сети Internet был полностью заблокирован на срок более 2 часов.

Будучи допрошенными по обстоятельствам дела К. и Х. пояснили, что они хотели «повалить сервер», руководствуясь исключительно желанием проверить свои способности к этому.

Решите вопрос об ответственности К. и Х.

3. Работник коммерческой организации Т., в обязанность которого входило техническое обслуживание компьютерной системы фирмы, из-за недобросовестного отношения к своим служебным обязанностям не проводил профилактики компьютеров, в частности периодических проверок на антивирусный контроль. В результате чего сроки технического обслуживания компьютеров были нарушены, в операционном зале постоянно не выдерживался температурный режим. Все это привело к сбою в работе компьютерной системы фирмы, что послужило основанием к прекращению её деятельности на несколько дней, чем фирме был причинен крупный материальный вред.

Как квалифицировать действия Т.?

Критерии оценивания решения практических задач

Отлично	Приведено правильное решение, учтены проблемные моменты вариантности решения, выявлены проблемные моменты, предложена и обоснована вариантность решения, ответ на задачу представляет собой логически построенный ответ, сочетающий теоретические знания и практическую материю задачи.
Хорошо	Приведено правильное решение (может содержать незначительные неточности).
Удовлетворительно	Неправильное решение, но теоретически обоснованное или правильное решение при слабом теоретическом обосновании.
Неудовлетворительно	Отказ от ответа или неправильное решение без обоснования.

Эссе

Примерный перечень тем эссе

1. Основы компьютерного законодательства США.
2. Internet – государство в государстве.
3. Ответственность за компьютерные преступления по уголовному законодательству государств-участников СНГ.
4. Понятие компьютерной информации.
5. Виды преступлений в сфере высоких технологий.
6. Особенности законодательной конструкции составов преступлений в сфере робототехники.
7. Характеристика основных групп способов совершения преступлений в сфере высоких технологий.
8. Зарубежный опыт классификации способов совершения преступлений в сфере высоких технологий.
9. Ответственность за несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины?
10. Внутренние пользователи: опасность изнутри компании.
11. Преступные последствия неправомерного доступа к компьютерной информации.
12. Специальный субъект неправомерного доступа к компьютерной информации.
13. Создание компьютерной программы как процесс написания её алгоритма.
14. Способы распространения вредоносных компьютерных программ.
15. Понятие «вируса».
16. Особенности формы вины при создании, использовании и распространении вредоносных компьютерных программ, повлекшие тяжкие последствия или создавших угрозу их наступления.
17. Правила эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации и информационно-телекоммуникационных сетей.
18. Правила эксплуатации информационно-телекоммуникационных сетей и оконечного оборудования.
19. Правила доступа к информационно-телекоммуникационным сетям.
20. Особенности субъектов компьютерных преступлений.
21. Хакер: компьютерный преступник или рядовой пользователь компьютерной техники?
22. Личностный аспект субъекта компьютерного преступления.
23. Робот как субъект компьютерного преступления.
24. Новейшие виды источников угроз информационной безопасности.
25. Мировой опыт противодействию преступлениям высоких технологий.
26. Правовое регулирование ответственности за мошенничество с использованием компьютерных технологий.
27. Состояние преступности в сфере компьютерной информации в РФ.
28. Качественная характеристика преступности высоких технологий в РФ.

Требования к эссе

1. Текст должен отражать позицию автора по какому-либо актуальному вопросу (проблеме). Автор должен высказать свою точку зрения и сформировать непротиворечивую систему аргументов, обосновывающих предпочтительность выбранной позиции.

2. В тексте должно быть продемонстрировано владение предметом исследования, его понятийным аппаратом, терминологией, знание общепринятых научных концепций в заданной предметной области, понимание современных тенденций и проблем в исследовании предмета.

3. Текст должен быть завершенным и четко структурированным, посвященным строго заданной выбранной темой проблематике.

4. Стилевое решение, структурная организация текста, лексика должны соответствовать заданной тематике и поставленной автором задаче.

5. Структура эссе: введение (в нем даётся краткая характеристика проблемной области по выбранной теме), основная (в ней раскрывается тема), заключение (в нем отражаются выводы по теме исследования, предложения о дальнейших работах в данной области и т.п.), список использованных ссылок и литературы (не менее 3).

6. Объем – не более 12000 знаков, шрифт Times New Roman прямого начертания, кегль (размер) шрифта 14, междустрочный интервал – полуторный.

Критерии оценки эссе

Критерий	Требования к эссе	Максимальное количество баллов
Знание и понимание теоретического материала	– рассматриваемые понятия определяются четко и полно, приводятся соответствующие примеры, – используемые понятия строго соответствуют теме, – самостоятельность выполнения работы.	1-10
Анализ и оценка информации	– грамотно применяется категория анализа, – умело используются приемы сравнения и обобщения для анализа взаимосвязи понятий и явлений, – объясняются альтернативные взгляды на рассматриваемую проблему, – обоснованно интерпретируется текстовая информация, – дается личная оценка проблеме с позиции эффективности осуществления предупреждения правонарушения, выявления и устранения причин и условий, способствующих их совершению.	1-10
Построение суждений	– изложение ясное и четкое, – приводимые доказательства логичны, – выдвинутые тезисы сопровождаются грамотной аргументацией, – приводятся различные точки зрения и их личная оценка, – общая форма изложения полученных результатов и их интерпретации соответствует жанру проблемной научной статьи с позиции эффективности осуществления предупреждения правонарушения, выявления и устранения причин и условий, способствующих их совершению.	1-10
Итоговая оценка	до 15 баллов – неудовлетворительно; 15-19 баллов – удовлетворительно; 20-25 баллов – хорошо; 26-30 баллов – отлично.	

Дискуссия.

Критерии оценивания дискуссии:

Оценка «5» (отлично) ставится, если: студент полно усвоил учебный материал; проявляет навыки анализа, обобщения, критического осмысления, публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации;

материал изложен грамотно, в определенной логической последовательности, точно используется терминология; показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; высказывать свою точку зрения; продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков.

Могут быть допущены одна – две неточности при освещении второстепенных вопросов.

Оценка «4» (хорошо) ставится, если: ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в усвоении учебного материала допущены небольшие пробелы, не исказившие содержание ответа; допущены один – два недочета в формировании навыков публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации.

Оценка «3» (удовлетворительно) ставится, если: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации.

Оценка «2» (неудовлетворительно) ставится, если: не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов; не сформированы компетенции, умения и навыки публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации

Тест.

Примерное тестовое задание

1. Первая электронно-вычислительная машина была создана:
А) в 1950 г.;
Б) в 1944 г.;
В) в 1954 г.;
Г) в 1940 г.
2. Термин «компьютерная преступность» впервые был введен:
А) в Германии;
Б) в Японии;
В) в США;
Г) во Франции.
3. Предметом компьютерного преступления является:
А) информация;
Б) компьютер;
В) охраняемая законом компьютерная информация;
Г) компьютерная система, компьютерная сеть.
4. Компьютерные преступления могут совершаться:
А) с прямым умыслом;
Б) с косвенным умыслом;
В) с преступной небрежностью;
Г) по неосторожности.
5. Какие из ученых посвятили свои монографические работы вопросам компьютерной преступности?
А) Гальперин И.М.;

Б) Карпец И.И.;
В) Батурин Ю.М.;
Г) Трайнин А.Н.

6. Глава 28 «Преступления в сфере компьютерной информации» включена законодателем в раздел УК РФ:

А) преступления в сфере экономики;
Б) преступления против общественной безопасности и общественного порядка;
В) преступления против правосудия;
Г) преступления против основ конституционного строя и безопасности государства.

7. Какие из перечисленных преступлений относятся к преступлениям в сфере высоких технологий?

А) разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну;
Б) неправомерный доступ к компьютерной информации;
В) изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов;
Г) отказ в предоставлении гражданину информации.

8. Родовым объектом преступлений в сфере компьютерной информации является:

А). компьютерная информация;
Б). общественная безопасность и общественный порядок;
В). общественная безопасность;
Г). компьютерная система или сеть.

9. Выберите наиболее верное определение понятию «компьютерная информация».

А) сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи;
Б) сведения о лицах, предметах, фактах, событиях и явлениях только ограниченного доступа, находящиеся на переносном электронном носителе;
В) сведения о лицах, предметах, фактах, событиях и явлениях, которые структурированы в единый каталог системы ограниченного пользования;
Г) сведения о лицах, предметах, фактах, событиях и явлениях неограниченного доступа, находящиеся в компьютере или в сети.

10. Объектом состава преступления, предусмотренного ст. 272 УК РФ являются:

А) отношения в сфере компьютерной безопасности;
Б) отношения в сфере обеспечения безопасности работы компьютера;
В) отношения в сфере охраны компьютерной информации;
Г) отношения в сфере создания и реализации компьютерных программ.

11. К методам несанкционированного доступа относятся:

А) «за дураком», «за хвост», «компьютерный абордаж», «неспешный выбор», «брешь», «маскарад», «мистификация», «аварийный», «склад без стен»;
Б) непосредственный перехват, электромагнитный перехват, аудиоперехват, видеоперехват, «мистификация», «аварийный», «склад без стен»;
В) «троянский конь», «за хвост», «логическая бомба», «неспешный выбор», «брешь», «маскарад», «асинхронная атака», «аварийный», «склад без стен»;
Г) «воздушный змей», «ловушка на живца», «компьютерный абордаж», «неспешный выбор», «брешь», «маскарад», «мистификация», «копирование», «склад без стен».

12. К законодательно установленным относятся следующие способы совершения преступлений в сфере компьютерной информации:

А) неправомерный доступ к охраняемой законом компьютерной информации;
Б) создание, использование и распространение вредоносных компьютерных программ;
В) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
Г) все указанное.

13. К обязательным признакам объективной стороны состава неправомерного доступа к компьютерной информации относятся:

А) неправомерный доступ к охраняемой законом компьютерной информации; общественно опасные последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации;

Б) общественно опасное деяние в виде неправомерного доступа к охраняемой законом компьютерной информации; общественно опасные последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации; причинная связь между совершенным общественно опасным деянием и наступившими общественно опасными последствиями;

В) неправомерный доступ к охраняемой законом компьютерной информации; общественно опасные последствия в виде нарушения работы средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; причинная связь между совершенным общественно опасным деянием и наступившими общественно опасными последствиями;

Г) общественно опасное деяние в виде неправомерного доступа к компьютерной информации; общественно опасные последствия в виде значительного ущерба; причинная связь между совершенным общественно опасным деянием и наступившими общественно опасными последствиями.

14. Укажите, какие общественно опасные последствия охватывает ст. 272 УК РФ?

А) уничтожение информации;

Б) модификация информации;

В) блокирование, копирование информации;

Г) все перечисленные ответы верны.

15. Данное определение: «запрещение дальнейшего выполнения последовательности команд или выключение из работы какого-либо устройства, или выключение реакции какого-либо устройства компьютера» характеризует процесс:

А) блокирования информации;

Б) уничтожения информации;

В) модификации информации;

Г) копированию информации.

16. Данное определение: «несанкционированная собственником или законным владельцем любая переработка первоначального состояния охраняемой законом информации, которая трансформирует ее содержание» характеризует процесс:

А) блокирования информации;

Б) уничтожения информации;

В) модификации информации;

Г) нарушения работы средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

17. Данное определение: «любой сбой вычислительной техники, препятствующий ее нормальному функционированию и находящийся в причинной связи с неправомерными действиями виновного лица при сохранении целостности компьютера, системы или их сети» характеризует процесс:

А) блокирования информации;

Б) уничтожения информации;

В) модификации информации;

Г) нарушения работы средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

18. К особо квалифицирующим признакам состава неправомерного доступа к компьютерной информации относятся следующие:

А) совершение группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения;

Б) повлекшее тяжкие последствия или создание угрозу их наступления;
В) причинившее крупный ущерб или совершенное из корыстной заинтересованности;
Г) повлекшее уничтожение, блокирование, модификацию либо копирование информации.

19. Субъекты компьютерных преступлений по уровню профессиональной подготовки подразделяются на:

А) рядовых пользователей и «белые воротнички»;
Б) взломщиков и вандалов;
В) компьютерных шпионов, хакеров;
Г) внутренних и внешних пользователей.

20. Неправомерный доступ к компьютерной информации может быть совершен:

А) с прямым умыслом;
Б) с косвенным умыслом;
В) по неосторожности;
Г) умышленно и по неосторожности.

21. Предметом состава создания, использования и распространения вредоносных компьютерных программ является:

А) охраняемая законом компьютерная информация;
Б) компьютер;
В) вредоносные компьютерные программы;
Г) компьютерная система, компьютерная сеть.

22. Каков по конструкции состав преступления, предусмотренного ст. 273 УК РФ?

А) материальный;
Б) формальный;
В) формально-материальный;
Г) усеченный.

23. Какие неправомерные действия предусматривает ст. 273 УК РФ?

А) создание компьютерных программ;
Б) использование компьютерных программ;
В) распространение компьютерных программ;
Г) похищение, создание, использование и распространение компьютерных программ.

24. Субъектом преступления, предусмотренного ст. 273 УК РФ является:

А) специальный субъект;
Б) общий субъект с 16 лет;
В) как специальный, так и общий;
Г) общий субъект с 14 лет.

25. Меры, направленные на предупреждение компьютерной преступности, подразделяются на следующие группы:

А) правовые, кадровые и технические;
Б) организационно-правовые и организационно-управленческие;
В) правовые и организационно-управленческие,
Г) морально-этические, физические и технические.

26. Правовой контроль над компьютерной преступностью подразделяется на:

А) позитивный и социальный;
Б) репрессивный и социальный;
В) позитивный и репрессивный;
Г) профилактический и карательный.

27. Определите вид диспозиции 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,»

А) описательная;
Б) бланкетная;
В) ссылочная;
Г) смешанная.

28. Субъект преступления ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» является:

А). общий, 16 лет;
Б). общий, 14 лет;
В). специальный – лицо, имеющее доступ к компьютеру, системе или их сети;
Г). специальный – должностное лицо.

29.По способу заражения компьютерной техники вирусы подразделяются на:

А) системные и файловые вирусы;
Б) резидентные и нерезидентные вирусы;
В) вульгарный и раздробленный вирус;
Г) файловые и комбинированные вирусы;
Г) морально-этические, физические и технические.

30. В каком нормативном правовом акте дается определение тяжких последствий, указанных в ч. 2 ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»

А). в УК РФ;
Б). в ФЗ "Об информации, информационных технологиях и о защите информации";
В). в четвертой части ГК РФ;
Г). понятие оценочное, определяет суд.

Критерии оценивания тестового задания

за правильный ответ - 1 балл;
если ответ не указан или не верен - 0 баллов

Оценка за итоговый контрольный тест по курсу выставляется в соответствии со следующими критериями:
Оценка «отлично» (5 баллов) - 81-100% правильных ответов
Оценка «хорошо» (4 балла) - 66-80% правильных ответов
Оценка «удовлетворительно» (3 балла) - 51 -65% правильных ответов
Оценка «неудовлетворительно» - 50% и менее правильных ответов.

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Форма промежуточной аттестации – зачет

Критерии выставления оценки на зачете.

Для получения зачета обучающийся должен получить не менее 25 баллов.

Баллы, начисляемые за работу магистра:

1. Посещение лекционных занятий – 1 балл за одно занятие, максимально 2 балла из расчета 2 лекций.

2. Посещение семинарских занятий - 2 балла за одно занятие, максимально 8 баллов из расчета 4 занятий.

3. Активность студента на занятии и качество его ответов (выступлений) - 5 баллов за одно занятие, максимально 20 баллов из расчета 4 занятий.

4. Выполнение домашних заданий (эссе) – максимально 5 баллов.

Итого максимально 35 баллов.

7. Перечень основной и дополнительной учебной литературы

7.1. Основная литература

1. Корабельников С.М. Преступления в сфере информационной безопасности: учебное пособие для вузов. Москва: Издательство Юрайт, 2022. 111 с. URL: https://urait.ru/book/prestupleniya-v-sfere-informacionnoy-bezopasnosti-448295

2. Бегишев И.Р. Преступления в сфере обращения цифровой информации: монография. Казань: Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с.URL: file:///C:/Users/Lopat/Downloads/cifrovaya-informaciya-begishev-bikeev.pdf

3. Криминология: учебник для бакалавриата, специалитета и магистратуры / под общ. ред. О. С. Капинус. 2-е изд., пер. и доп. Москва: Издательство Юрайт, 2019. – 1132 с.URL: https://urait.ru/book/kriminologiya-428579

4. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / ответственные редакторы С. В. Зуев, В. Б. Вехов. Москва: Издательство Юрайт, 2021. 243 с. URL: https://urait.ru/bcode/467208 (дата обращения: 06.05.2022).https://urait.ru/book/rassledovanie-prestupleniy-v-sfere-kompyuternoy-informacii-i-elektronnyh-sredstv-platezha-467208

7.2. Дополнительная литература

1. Воронин Ю.А. Преступления в сфере обращения цифровой информации и их детерминанты // Виктимология. – 2020. – № 1 (23). – С. 74–80. URL: https://elibrary.ru/item.asp?id=42768187

2. Грачева Ю.В. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения // Lex russica (Русский закон). – 2020. – № 1 (158). – С. 145-159. URL: https://elibrary.ru/item.asp?id=42335041

3. Генпрокурор России Игорь Краснов провел совещание по теме борьбы с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news/archive?item=56766040

4. Главы МВД стран ШОС в Душанбе обсудят вопросы борьбы с киберпреступностью. URL: https://tj.sputniknews.ru/20150605/1015661454.html .

5. Десять самых разрушительных вирусов в истории. URL: https://habr.com/ru/post/4141/.

6. Доктор Веб: обзор вирусной активности за 2020 год. URL: https://news.drweb.ru/show/review/?lng=ru&i=14108.

7. Европол. Киберстратегия // Европол: официальный сайт. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

8. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография. – Москва: Юрлитинформ, 2018. – 312 с. URL: https://elibrary.ru/item.asp?id=30081476

9. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект).

10. Kaspersky Security Bulletin 2020: Киберугрозы для финансовых организаций в 2021 году. URL: https://securelist.ru/cyberthreats-to-financial-organizations-in-2021/99420/

11. Мосечкин И.Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования: монография. – Киров: Вятский государственный университет, 2020. – 111 с. URL:https://elibrary.ru/item.asp?id=42968607

12. Поляков И.В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. – 2020. – № 4. – С. 21-25. URL: https://elibrary.ru/item.asp?id=44449876

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

I. Сайты базовых академических и государственных структур

1. Генеральная прокуратура РФ // http://www.genproc.gov.ru
2. Верховный Суд Российской Федерации // http://www.supcourt.ru
3. Сайт МВД РФ // http://www.mvdinform.ru
4. Юридическая Россия. Федеральный портал // http://www.law.edu.ru
5. Научная литература по юридическим дисциплинам // Академия Google // scholar.google.com
6. Поиск научной информации для ученых, специалистов, аспирантов, студентов // http://www.scholar.ru
7. Юридический портал «Правопорядок»: электронная юридическая библиотека, 2011. – Режим доступа: http://www.oprave.ru.

II. Электронные библиотеки

1. ЭБС «Юрайт» https://urait.ru/.
2. Научная электронная библиотека: http://elibrary.ru.

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, (полигон, класс криминалистики)

214000, г. Смоленск, ул. Пржевальского, д.4, уч. корпус № 1, ауд.71
Учебная мебель
(30 учебных посадочных мест), стол и стул для преподавателя – по 1 шт.
Кафедра для лектора 1 шт.
Мультимедийный проектор BenQ -1 шт.
Криминалистические стенды

Помещение для самостоятельной работы
214000, г. Смоленск, ул. Пржевальского, д.4, уч. корпус №1, ауд.12 б
Компьютерный класс с выходом в Интернет
Учебная мебель (47 посадочных мест), компьютерный класс с выходом в сеть Интернет (18 компьютеров)
Интерактивная доска SMART
Мультимедийный проектор
Сканер формат A3EpsonGT – 20000
Принтер формат А3 Е 100
Компьютерное оборудование Kraftway КС 41

9. Перечень информационных технологий

1. Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия66920993от 24.05.2016, (бессрочно)
2. Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия66975477от 03.06.2016, (бессрочно)
3. KasperskyEndpointSecurity для бизнеса – Стандартный, Лицензия 1FB6181220135520512073, ежегодное обновление