МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

СОГЛАСОВАНО
Руководитель ОП

Р.И. Дремлюга

«17» июня .2019 г.

УТВЕРЖДАЮ
Директор Школы цифровой экономики

_____И.Г. Мирин

«17» _____2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«КОМПЬЮТЕРНЫЕ ПРАВОНАРУШЕНИЯ И ИНЦИДЕНТЫ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

курс 2 семестр 4
лекции 18 час.
практические занятия 18 час.
лабораторные работы 0 час.
всего часов аудиторной нагрузки 36 час.
самостоятельная работа 72 час.
контрольные работы программой не предусмотрены
курсовая работа/проект – не предусмотрено
зачет 4семестр
экзамен – не предусмотрено учебным планом

Рабочая программа составлена в соответствии составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918.

Рассмотрена и утверждена на заседании Дирекции Школы цифровой экономики «17» июня 2019 года (протокол № 124-01-07-05).

Составитель: к.ю.н. Р.И. Дремлюга

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ

Б1.В.ДВ.01.11 КОМПЬЮТЕРНЫЕ ПРАВОНАРУШЕНИЯ И ИНЦИДЕНТЫ

Учебный курс «Компьютерные правонарушения и инциденты» предназначен для студентов, обучающихся по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры), профиль «Кибербезопасность».

Дисциплина «Компьютерные правонарушения и инциденты» входит в часть, формируемую участниками образовательных отношений, блока «Дисциплины (модули) Б1» (Б1.В.ДВ.01) учебного плана подготовки магистров, модуль элективных дисциплин

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы или 108 часов. Дисциплина реализуется на 2 курсе в 4 семестре.

Семестр	Аудиторные Занятия			Самостоятель-ная работа	Контроль	Форма контроля	Всего по дисциплине	
	Лекции	Лабораторные заня-тия	Практические занятия				Часы	з.е.
4 семестр	18	-	18	72		зачет	108	3

Целью изучения дисциплины «Компьютерные правонарушения и инциденты» является овладение обучающихся теоретическими и практическими основами применения компьютерной технологии и компьютерной техники при расследовании компьютерных преступлений и экспертной деятельности.

В результате освоения дисциплины обучающийся приобретает следующие навыки:

Знать основные законодательные акты и нормативные документы, связанные со следственной практикой и судебной экспертизой;

Уметь использовать законодательные акты и нормативные документы, связанные с осмотром компьютерной техники и поиском, исследованием и изъятием электронной информации в профессиональной деятельности;

Владеть приемами проведения следственных действий применительно к информационным системам.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции:

Код и формулировка компетенции	**Этапы формирования компетенции**
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	ПК-4.1 Знает: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях ПК-4.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-4.3 Владеет навыками: анализа защищенности компьютерных систем с использованием сканеров безопасности и защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок
ПК-5 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-5.1 Знает: форматы хранения информации в анализируемой компьютерной системе; особенности хранения конфигурационной и системной информации в компьютерных системах; уязвимости компьютерных систем и сетей; порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; нормы уголовного и административного права в сфере компьютерной информации; характеристики правонарушений в области связи и информации; виды преступлений в сфере компьютерной информации; порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов ПК-5.2 Умеет: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; выявлять возможные траектории состояний

	функционирования системы и несоответствия имеющейся информации ее расположению в системе ПК-5.3 Владеет: технологиями поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; навыками прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов; способами обнаружения и нейтрализации последствий вторжений в компьютерные системы; методами анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов; методами анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении
ПК-6 Способен разрабатывать и тестировать средств защиты информации компьютерных систем и сетей	ПК-6.1 Знает: принципы проектирования антивирусного программного обеспечения; виды атак и механизмы их реализации в компьютерных системах; принципы построения систем защиты информации компьютерных систем; методологии и технологии разработки программного и аппаратного обеспечения; криптографические алгоритмы и особенности их программной реализации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации ПК-6.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-6.3 Владеет методами и средствами получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях; защиты информации в компьютерных сетях, операционных системах и системах управления базами данных; анализа безопасности компьютерных систем

Для формирования вышеуказанных компетенций в рамках дисциплины «Компьютерные правонарушения и инциденты» применяются следующие методы активного / интерактивного обучения: работа в малых группах (дает всем студентам возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения); видеоанализ; эссе; метод ситуационного анализа (ситуационные задачи); тестирование, реферат.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекции и практические занятия (36 час.)

Семинар 1. Понятие информационных преступлений

Вопросы для обсуждения:

1. Понятие и виды информационных преступлений.
2. Классификация информационных преступлений.
3. Выявление конкретных составов информационных преступлений, содержащихся в УК РФ.
4. Сравнительный анализ компьютерных преступлений как одного из основных видов информационных преступлений.
5. Формулирование предложений по совершенствованию уголовного законодательства в области регулирования информационных преступлений.

Семинар 2. Криминалистическая характеристика преступлений в сфере компьютерной информации

Вопросы для обсуждения:

1. Структурные элементы криминалистической характеристики преступлений в сфере компьютерной информации и высоких технологий.
2. Способы подготовки, совершения и сокрытия преступлений.
3. Личность преступника.

Семинар 3. Компьютерно-техническая экспертиза

Вопросы для обсуждения:

1. Понятие компьютерно-технической экспертизы.
2. Вопросы для эксперта.
3. Исследование носителей информации.
4. Технические и программные средства проведения КТИ.
5. Экспертные инструменты и авторское право.

Семинар 4. Отдельные вопросы расследования и предупреждения информационных преступлений

Вопросы для обсуждения:

1. Методика расследования информационных преступлений.
2. Корректность и неизменность информации при изъятии.
3. Общие правила изъятия компьютерной техники при обыске.
4. Особенности работы следователя с доказательственной информацией:

- на ноутбуках;
- на КПК;
- на флэш-накопителях;
- на мобильных телефонах и коммутаторах;
- на автомобильных видеорегистраторах, цифровых фотоаппаратах.

4. Предупреждение компьютерных преступлений.
5. Особенности предупреждения информационных преступлений в информационно-телекоммуникационной сети Интернет.

Планы практических занятий

Практическое занятие 1. Вводное

План занятия:

1. Структура, особенности, цели и актуальность учебной дисциплины «Форенсика».
2. Формы контроля успеваемости студентов по учебной дисциплине.
3. Порядок работы студента на лекциях, семинарах.

Практическое занятие 2. Отдельные виды информационных преступлений

План занятия:

1. Онлайн-мошенничество.
2. Клевета, оскорбления и экстремистские действия в Сети.
3. Вредоносные программы.
4. Скиминг.
5. Посреднические онлайн-сервисы.
6. Нарушение авторских прав.

7. Фишинг. Кибersквоттинг.

8. Платежи через Интернет.

Практическое занятие 3. Характеристика исходных данных об информационном преступлении

План занятия:

1. Способы воздействия на информацию при совершении преступлений.

2. Система материальных и идеальных следов компьютерных преступлений.

3. Сведения о предполагаемой личности преступника.

Практическое занятие 4. Место и роль компьютерно-технической экспертизы в расследовании информационных преступлений

План занятия:

1. Проблемы назначения эксперта.

2. Проблемы с постановкой вопросов эксперту.

3. Влияние фактора времени на КТЭ.

4. Взаимодействие с пользователем.

5. Стоимость КТЭ.

Практическое занятие 5. Типичные следственные ситуации на первоначальном этапе расследования преступлений в сфере информации

План занятия:

1. Выдвижение следственных версий в зависимости от исходной информации.

2. Программно-техническое обеспечение процесса подготовки и производства следственных действий.

3. Тактика производства отдельных следственных действий.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Компьютерные проавонарушения и инциденты» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые модули/ разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				Текущий контроль	Промежуточная аттестация
1.	Занятия 1-9	ПК-4 ПК-5 ПК-6	Знает	УО-2 (коллоквиум)	УО-1 (собеседование), вопросы к зачету: № 1-60
			Умеет	ПР-1 (тест)	
			Владеет	ПР-11 (разноуровневые задачи)	ПР-11 (разноуровневые задачи)

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Калмыков, И. А. Компьютерная криминалистика [Электронный ресурс] : лабораторный практикум / И. А. Калмыков, В. С. Пелешенко. — Электрон. текстовые данные. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 84 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69392.html

2. Криминалистика : учебник для вузов / Н. П. Яблоков ; Московский государственный университет, Юридический факультет. Москва : Норма, : Инфра-М, 2015. 399 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:795350&theme=FEFU

3. Криминалистика: курс лекций : учебное пособие для вузов / Р. А. Адельханян, Д. И. Аминов, П. В. Федотов. Москва : Юнити-Дана, 2014. 239 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:725025&theme=FEFU

4. Криминалистика сборник задач [Электронный ресурс]. Ставрополь: Северо-Кавказский федеральный университет, 2015. 82 с. http://www.iprbookshop.ru/62948.html

5. Криминалистика [Электронный ресурс]: Учебное пособие [Электронный ресурс] / Балашов Д. Н., Балашов Н. М., Маликов С. В. - 6 изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2015. - 241 с. http://znanium.com/catalog/product/460715

Дополнительная литература

(печатные и электронные издания)

1. Криминалистика : учебник / [О. В. Волохова, Н. Н. Егоров, М. В. Жижина и др.] ; под ред. Е. П. Ищенко. Москва : Проспект, 2014. 501 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:739018&theme=FEFU

2. Введение в криминалистику и криминалистическое образование [Электронный ресурс] / М.К. Каминский. Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2015. 44 с. http://www.iprbookshop.ru/69342.html

3. Курс лекций по криминалистике для бакалавров: учебное пособие [Электронный ресурс] / М.К. Каминский, А.М. Каминский. Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2015. 332 с. http://www.iprbookshop.ru/69357.html

4. Информатизация криминологической деятельности. Теория и методология: монография / А.Я. Минин. М.: Московский педагогический государственный университет, 2015. 168 с. http://www.iprbookshop.ru/70002.html

Нормативно-правовые материалы

1. Конституция Российской Федерации от 12.12.93 (с поправками) // Рос. газета. 1993 г. 25 декабря // Справочно-правовая система Консультант Плюс http://www.consultant.ru/document/cons_doc_LAW_28399/

2. Уголовный кодекс Российской Федерации // Справочно-правовая система Консультант Плюс http://www.consultant.ru/document/cons_doc_LAW_10699/

3. Уголовно-процессуальный кодекс Российской Федерации // Справочно-правовая система Консультант Плюс http://www.consultant.ru/document/cons_doc_LAW_34481/

4. Уголовно-исполнительный кодекс Российской Федерации // Справочно-правовая система Консультант Плюс http://www.consultant.ru/document/cons_doc_LAW_12940/

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Информационно-библиотечная база данных ДВФУ предоставляет возможность неограниченного доступа к следующим электронным ресурсам:

1. Электронная библиотека диссертаций РГБ http://diss.rsl.ru/;
2. Научная электронная библиотека (НЭБ) http://elibrary.ru/defaultx.asp?;
3. Электронно-библиотечная система znanium.com НИЦ "ИНФРА-М" http://znanium.com/;
4. Электронно-библиотечная система IPRbooks http://www.iprbookshop.ru/;
5. Электронно-библиотечная система издательства "ЮРАЙТ" http://www.biblio-online.ru/home;jsessionid=31138d119c6575d963c72d3e0c93?0
6. Сайт Верховного суда Российской федерации: www.vsrf.ru;
7. Сайт Генеральной прокуратуры Российской Федерации: www.genproc.gov.ru;
8. Сайт Министерства внутренних дел Российской Федерации: www.mvd.ru;
9. Сайт Следственного комитета Российской Федерации: www.sledcom.ru

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Основными видами занятий при изучении дисциплины «Компьютерные проавонарушения и инциденты» являются практические (семинарские) занятия.

Практические (семинарские) занятия проводятся в целях закрепления теоретических положений законодательства, обобщения судебной практики и обсуждения мнений ученых-теоретиков.

Особо значимой для профессиональной подготовки студентов является *самостоятельная работа* по курсу. В нее входит: подготовка к практическим занятиям, решение практических (ситуационных) задач, подготовка к зачету.

Для более глубокой проработки вопросов каждой темы практического (семинарского) занятия студенту рекомендуется использовать рекомендованные источники в списке нормативного материала, судебной практики и литературы, нормативные акты, а также следить за изменениями законодательства и анализировать судебную практику, связанную с криминалистической деятельностью.

Практические занятия проводятся с группой и строятся как беседа-дискуссия по каждому вопросу плана. При изучении курса необходимо прорабатывать темы в той последовательности, в которой они даны в программе и планах практических занятий. Проработку каждого из вопросов целесообразно начинать со знакомства с содержанием соответствующего раздела программы курса и обращения к обозначенным в списке литературы источникам.

Методы проверки знаний студентов:

1. Коллоквиум (УО-2) – средство контроля усвоения учебного материала организованное как учебное занятие в виде собеседования преподавателя с обучающимися.

2. Тестирование (ПР-1), которое позволяет проверить наличие у студентов сформировавшегося понятийного аппарата. Поскольку при тестировании от студента требуется выбрать правильный ответ из нескольких вариантов, преимуществом этого метода является также простота оценки результатов. Решение заданий в форме тестов представляет собой определенный тренинг, который способствует активизации мышления и закрепления в памяти студентов юридических понятий и терминов и другой информации.

3. Решение практических (ситуационных) задач (ПР-11), которое показывает степень формирования у студентов практических навыков.

Решение задач является традиционным и важнейшим методом проведения практических занятий, поэтому следует более детально остановиться на рассмотрении основных подходов к решению задач.

В процессе решения задач осваиваются алгоритмы юридического мышления, без овладения которыми невозможно успешное решение практических проблем. Эти алгоритмы включают в себя:

1) изучение конкретной ситуации (отношения), требующей правового обоснования или решения;

2) правовая оценка или квалификация этой ситуации (отношения);

3) поиск соответствующих нормативных актов и судебной практики;

4) толкование правовых норм, подлежащих применению;

5) принятие решения, разрешающего конкретную заданную ситуацию;

6) обоснование принятого решения, его формулирование в письменном виде;

7) проецирование решения на реальную действительность, прогнозирование процесса его исполнения, достижения тех целей, ради которых оно принималось.

Условия задач включают все фактические обстоятельства, необходимые для вынесения определенного решения по спорному вопросу, сформулированному в тексте задачи. Решение задачи необходимо записывать в тетрадь, предназначенную для внесения подобного рода записей. При решении задачи ее условие переписывать не нужно; достаточно указать номер задачи, а затем сформулировать свои ответы на поставленные в задаче вопросы.

К тексту задачи обязательно прикладываются фотографии (рисунки) с мест происшествий, а также фотографии (рисунки) подозреваемых (обвиняемых) и потерпевших. Студенту необходимо внимательно исследовать эти фотографии (рисунки) с целью ответить на поставленный вопрос (ы) в задаче.

В ответе на поставленный в задаче вопрос (вопросы) необходимо дать обоснованную оценку предложенной ситуации с точки зрения действующего законодательства. При решении задач недопустимо ограничиваться однозначным ответом «да» или «нет».

Формой итогового контроля знаний студентов выступает зачет (6 семестр).

К зачету по дисциплине «Компьютерные проавонарушения и инциденты» необходимо начинать готовиться с первого занятия (лекции, практического занятия). В подготовку входит повторение пройденного материала. Для упрощения процесса подготовки рекомендуем подготовить и записать ответы на вопросы, а также отметить наиболее трудные, которые вызывают сложности при подготовке.

В подготовку к зачету ходит повторение пройденного материала. Для упрощения процесса подготовки рекомендуем подготовить и записать ответы на вопросы, а также отметить наиболее трудные, которые вызывают сложности при подготовке. Также целесообразно делать к каждой теме словарь основных терминов (понятий) курса.

Зачет проводится в форме устного опроса – собеседования (УО-1).

Собеседование (УО-1) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Устный опрос (собеседование) проходит с предварительной подготовкой студентов (не более 40 минут). Также в ходе проверки практических навыков освоения дисциплины «Криминалистика» студентам необходимо решить практическую задачу (на ее решение отводится до 40 минут).

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения данной дисциплины необходима аудитория, оснащенная презентационной техникой, компьютерный класс с программным обеспечением и возможностью использования Интернет-ресурсов, учебные и методические пособия (учебники, программы, сборники упражнений и т.д.), расходные материалы (бумага, картридж).

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебная аудитория для занятий семинарского типа 690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10 Здание ФЭК корпус А, лит О, ауд. G468	Комплект специализированной мебели: доска аудиторная – 1 шт.; парты – 30 шт.; стул -30 шт.; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi; Системный блок с монитором. Процессор: Intel I5-8600k 3.6Ghz, оперативная память: 32gb, жесткий диск: 1ТБ, графический ускоритель: Nvidia GTX 1080 Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS).

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине

«КОМПЬЮТЕРНЫЕ ПРОАВОНАРУШЕНИЯ И ИНЦИДЕНТЫ»

направления 09.04.01 Информатика и вычислительная техника

Магистерская программа «Кибербезопасность»

Форма подготовки очная

Владивосток
2018

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка практических заданий.	40	Отчет по самостоятельной работе
2	Сессия	Подготовка к зачету	20	Зачет

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;

- умение сформировать свою позицию, оценку и аргументировать ее

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	**Оценка**
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по практическим занятиям и лабораторным работам.

Примерные темы рефератов и эссе

1. Правовое обеспечение компьютерной безопасности как элемент информационной безопасности.
2. Организационно-техническое обеспечение компьютерной безопасности как элемент информационной безопасности.
3. Компьютерные преступления как обособленная группа общественно-опасных деяний.
4. Криминалистическая характеристика компьютерных преступлений.
5. Обнаружение, фиксация и изъятие следов компьютерных преступлений.
6. Основы тактики проведения отдельных следственных действий по делам о компьютерных преступлениях.
7. Силы оперативно-розыскной деятельности, используемые при предупреждении и раскрытии компьютерных преступлений.

8. Основания и условия проведения оперативно-розыскных мероприятий при предупреждении и раскрытии компьютерных преступлений.

9. Использование результатов, полученных при проведении оперативно-розыскных мероприятий в процессе раскрытия и расследования компьютерных преступлений.

10. Основы организации и методики проведения компьютерно-технических экспертиз.

Методические рекомендации по решению задач

Для правильного решения задач по конкретной теме студент должен предварительно изучить действующее законодательство, иной нормативно-правовой материал по теме, относящийся как к криминалистике, так и к другим отраслям права, соответствующие постановления Пленумов Верховного Суда РФ, лекционный и учебный материалы, монографическую литературу, научные статьи и комментарии. Решение задач на практическом занятии состоит в изложении студентом обстоятельств дела, основного вопроса задачи, вопросов, от которых зависит решение, ответов на них. Решение должно быть развернутым, последовательным, аргументированным, подкрепленным ссылками на фактические обстоятельства дела, нормы уголовного права, иной нормативный материал. Ответ на вопрос задачи предполагает доказывание студентом избранного им решения.

При решении задачи необходимо уяснить содержание задачи и все обстоятельства дела, а также внимательно проанализировать доводы конфликта и дать им оценку с точки зрения действующего законодательства.

К тексту задачи обязательно прикладываются фотографии (рисунки) с мест происшествий, а также фотографии (рисунки) подозреваемых (обвиняемых) и потерпевших. Студенту необходимо внимательно исследовать эти фотографии (рисунки) с целью ответить на поставленный вопрос (ы) в задаче.

Помимо этого, необходимо ответить на теоретические вопросы, поставленные в задаче в связи с предложенной ситуацией.

Решение задачи должно содержать:

- краткое изложение обстоятельств дела;
- юридическая оценка юридического дела;
- ссылки на конкретные нормы уголовного закона или иного правового акта по рассматриваемому делу;
- выводы и их обоснование по постановленному в задаче вопросу.

При решении задач недопустимо ограничиваться однозначным ответом «да» или «нет».

Решение практических (ситуационных) задач оформляется в письменном виде и сдается на проверку преподавателю.

Приложение 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
«КОМПЬЮТЕРНЫЕ ПРАВОНАРУШЕНИЯ И ИНЦИДЕНТЫ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	ПК-4.1 Знает: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях ПК-4.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-4.3 Владеет навыками: анализа защищенности компьютерных систем с использованием сканеров безопасности и защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок
ПК-5 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-5.1 Знает: форматы хранения информации в анализируемой компьютерной системе; особенности хранения конфигурационной и системной информации в компьютерных системах; уязвимости компьютерных систем и сетей; порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; нормы уголовного и административного права в сфере компьютерной информации; характеристики правонарушений в области связи и информации; виды преступлений в сфере компьютерной информации; порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов ПК-5.2 Умеет: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; выявлять возможные траектории состояний функционирования системы и несоответствия имеющейся информации ее расположению в системе ПК-5.3 Владеет: технологиями поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; навыками прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов;

	способами обнаружения и нейтрализации последствий вторжений в компьютерные системы; методами анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов; методами анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении
ПК-6 Способен разрабатывать и тестировать средств защиты информации компьютерных систем и сетей	ПК-6.1 Знает: принципы проектирования антивирусного программного обеспечения; виды атак и механизмы их реализации в компьютерных системах; принципы построения систем защиты информации компьютерных систем; методологии и технологии разработки программного и аппаратного обеспечения; криптографические алгоритмы и особенности их программной реализации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации ПК-6.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-6.3 Владеет методами и средствами получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях; защиты информации в компьютерных сетях, операционных системах и системах управления базами данных; анализа безопасности компьютерных систем

Контроль достижения целей курса

№ п/п	Контролируемые модули/ разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				Текущий контроль	Промежуточная аттестация
1.	Занятия 1-9	ПК-4 ПК-5 ПК-6	Знает	УО-2 (коллоквиум)	УО-1 (собеседование), вопросы к зачету: № 1-23
			Умеет	ПР-1 (тест)	
			Владеет	ПР-11 (разноуровневые задачи)	ПР-11 (разноуровневые задачи)

Примерные вопросы для подготовки к зачету

1. Понятие информационного преступления.
2. Классификация информационных преступлений.
3. Понятие криминалистической характеристики преступлений в сфере компьютерной информации.
4. Особенности формирования криминалистической характеристики информационных преступлений.
5. Характеристика исходной информации о преступлении.
6. Значение исходной информации об информационных преступлениях в криминалистической характеристике.
7. Способы воздействия на информацию при совершении преступлений.
8. Система материальных и идеальных следов компьютерных преступлений.
9. Сведения о предполагаемой личности преступника.
10. Криминалистическая характеристика онлайн-мошенничества.
11. Криминалистическая характеристика DoS-атаки.
12. Вредоносные программы.
13. Криминалистическая характеристика фишинга.
14. Место и роль компьютерно-технической экспертизы в расследовании информационных преступлений.
15. Проблемы назначения компьютерно-технических экспертиз.
16. Типичные следственные ситуации на первоначальном этапе расследования преступлений в сфере информации.
17. Выдвижение следственных версий при расследовании информационных преступлений.
18. Программно-техническое обеспечение процесса подготовки и производства следственных действий.
19. Тактика производства осмотра машинных носителей информации.

20. Тактика производства осмотра (обыска) средств компьютерной техники.

21. Правовые меры предупреждения компьютерных преступлений.

22. Организационно-технические меры предупреждения информационных преступлений.

23. Вопросы контроля за Интернет-средой.

Примерный вариант тестовых заданий

1. Природа науки киберкриминалистики:

1) техническая;
2) юридическая;
3) интегративная;
4) техническая и юридическая (двойственная природа).

2. Предмет криминалистики – это:

1) закономерности механизма преступления, возникновения информации о преступлении и его участниках, собирания, исследования и использования доказательств и основанные на познании этих закономерностей специальные методы и средства судебного исследования и предотвращения преступлений;
2) система приемов и методов по раскрытию и расследованию преступлений;
3) научное понятие, включающее: введение в криминалистику, криминалистическую технику, криминалистическую тактику и криминалистическую методику;
4) закономерности предупреждения преступлений.

3. Задачами криминалистики являются:

1) содействие правоохранительным органам в борьбе с преступностью; познание объективных закономерностей, составляющих основу предмета науки; совершенствование технико-криминалистического обеспечения расследования преступлений; разработка и совершенствование организационных, тактических и методических основ предварительного и судебного следствия; изучение и обобщение следственной и судебной практики; разработка криминалистических средств и методов предотвращения преступлений, использование в расследовании преступлений достижений зарубежных криминалистов;
2) разработка новых и совершенствование тактических приемов проведения следственных действий;

3) разработка новых и совершенствование имеющихся технико-криминалистических средств и методов собирания, и исследования доказательств;
4) совершенствование имеющихся и разработка новых методик расследования и предупреждения различных видов преступлений.

4. Систему науки криминалистики составляют следующие элементы:
1) криминалистическая методика, криминалистическая тактика, криминалистическая экспертиза, криминалистическая техника;
2) криминалистическая техника, организация расследования преступлений, методологические основы криминалистики;
3) общая теория криминалистики (методологические основы), криминалистическая техника, криминалистическая тактика, криминалистическая методика;
4) организация расследования преступлений, методологические основы, криминалистическая техника, криминалистические версии, криминалистическая тактика, криминалистическая методика.

5. К специальным методам науки криминалистики относятся:
1) наблюдение, сравнение, эксперимент;
2) измерение, сопоставление, описание;
3) сравнение, описание, моделирование, наблюдение;
4) методы криминалистической идентификации, дактилоскопии, одорологии, планирования расследования.

6. Кем совершаются преступления в сфере компьютерной информации?
А)ЭВМ
Б)компьютерной сетью Интернет
В)человеком
Г)таких преступлений не существует

7. Преступления в сфере информационных технологий включают:
А) распространение вредоносных вирусов
Б) неправильно выключить компьютер
В) кражу номеров кредитных карточек
Г) украсть книжку из библиотеки
Д) взлом паролей

Е) распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет.

8. По УК РФ преступлениями в сфере компьютерной информации являются:

А) неправомерный доступ к компьютерной информации

Б) Создание, использование и распространение вредоносных компьютерных программ

В) Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации

Г) кража компьютера из офиса

Д) сломать кредитную карточку по неосторожности

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

А) могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов

Б) серьёзное нарушение работы ЭВМ и их систем

В) несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов

Г) замыкание электросети и электроприборов

10. В каком нормативно правовом акте можно найти санкции за данный вид преступления?

А) Конституция РФ

Б)Конституция РБ

В)Гражданский кодекс РФ

Г) Уголовный кодекс РФ

11. Первые преступления с использованием компьютерной техники в России появились:

А) в 1991г.

Б) в 2000

В) В 2012

Г) нет таких

12. Виды изменения компьютерных данных:

А) логическая бомба

Б) троянский конь
В) компьютерный вирус
Г) приложение

13. Виды компьютерных преступлений:

А) изменение компьютерных данных
Б) компьютерное мошенничество
В) компьютерное пиратство
Г) прослушивание музыки онлайн

Пример практические задания

Перечень типовых заданий
1.В квартире проживали 4 человека и имелся 1 компьютер. Компьютером 1 января с 19.00 - 21.00 периодически подходили каждый из проживающих. В 20.00 было совершено преступление - неправомерный удаленный доступ к аккаунту в социальной сети посредством подбора пароля. В результате произошло ознакомление с личной информацией, ее копирование, а также рассылка текстовых сообщений от имени потерпевшего. По предварительным данным стало известно, что способ совершения преступления включал в себя следующие действия: использование эксплойта для получения доступа к компьютеру потерпевшего, внедрение в него ВПО, выполняющего поиск документов с паролями, подбор паролей, копирование и пересылка полученной информации в облачное хранилище. Каждый из проживающих в квартире отрицает свое участие в преступлении, но соглашается с тем, что в период с 19.00 - 21.00 он, как и остальные, мог пользоваться компьютером, в частности, заходить в социальные сети, использовать текстовые и графические редакторы, искать и просматривать информацию в сети Интернет и пр. Вопросы. Что способствовало совершению преступления? Опишите недостающие данные по способу совершения преступления? Какие средства использовались в данном преступлении? Какие следы в данной ситуации могут находиться в компьютере, а также какие из них могут персонифицировать преступника?

Оценивание выполнения практических заданий

4-балльная шкала	**Критерии**
Отлично	Студентом задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом.

Хорошо	Студентом задание решено с подсказкой преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.
Удовлетворительно	Студентом задание решено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задание решено не полностью или в общем виде.
Неудовлетворительно	Студентом задание не решено.

Оценивание выполнения тестов

4-балльная шкала	**Критерии**
Отлично	выполнено 85-100 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос;
Хорошо	выполнено 70-84 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответна поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.
Удовлетворительно	выполнено 30-69 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
Неудовлетвори-тельно	выполнено 1 – 29 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Оценивание ответа на зачете

Бинарная шкала	Критерии
Зачтено	Студентом даны развернутые ответы на поставленные вопросы, где студент демонстрирует приобретенные знания, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа.
Не зачтено	Студентом даны ответы, которые содержат ряд серьезных неточностей, обнаруживающие незнание процессов изучаемой предметной области, отличающиеся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической

	речью, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.