МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования

**«Российский государственный
университет социальных технологий»**

(ФГБОУ ИВО «РГУ СоцТех»)

УТВЕРЖДАЮ

Проректор по образовательной деятельности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
КИБЕРПРЕСТУПНОСТЬ И КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА
образовательная программа направления подготовки
09.04.03 «Прикладная информатика»
Б1.В.ДВ.02.02 «Дисциплины(модули)», Часть, формируемая участниками образовательных отношений, Дисциплины(модули) по выбору

Профиль подготовки
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:
Магистр

Форма обучения очная

Курс 2 семестр 3

Москва 2024

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Цель курса состоит в получении студентами прочных теоретических знаний и практических навыков в области киберпреступности и компьютерной криминалистики

Задачи дисциплины:

1. изучение методологических подходов и основных принципов компьютерной криминалистики;
2. определение места компьютерной криминалистики в криминалистике
3. криминалистическая характеристика компьютерных преступлений. Определение основных групп компьютерных преступлений.
4. изучение видов и способовв проведения компьютерной экмпертизы
5. освоение применения основных принципов защиты от киберпреступности;
6. получение навыков использования различных методов в профессиональной деятельности.

Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-3 Способен разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач проектной деятельности	ПК-3.1. Знает языки программирования, библиотеки и пакеты программ; современные методы цифровой обработки изображений и средства компьютерной обработки информации.
	ПК-3.2. Умеет анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи.
	ПК-3.3. Владеет методами моделирования информационных процессов; навыками работы над проектом в составе группы научных специалистов, различными методами осуществления компьютерной криминалистики
ПК-7 Способен проектировать архитектуру ИС предприятий и организаций в прикладной области	ПК-7.1 Знает процесс подготовки информации к принятию управленческих решений систему сбора, обработки и подготовки информации по предприятию и его структурным подразделениям; виды и особенности архитектур и сервисов ИС предприятий и организаций в прикладной области; методы оценки экономической эффективности и качества информационных систем, в т.ч. для учета проектных рисков.
	ПК-7.2 Умеет формировать общий бюджет предприятия в разрезе его составных частей; подготовить релевантную информацию для принятия решения
	ПК-7.3 Владеет навыками использования современных инструментальных средств при разработке ИС различного назначения; практическими навыками проектирования архитектуры информационных систем и сервисов на основе современных методов и технологий; практическими навыками использования современных инструментальных средств в области компьютерной криминалистики .
ПК-9 Способен принимать эффективные проектные решения в условиях неопределенности и риска	ПК-9.1 Знает принципы, методы, положения, определения эффективности проектных решений в условиях неопределенности и риска; возможности современных инструментальных средств для анализа, моделирования, оценки информационных процессов предприятий прикладной области в условиях неопределенности и риска.

	ПК-9.2 Умеет решений в условиях неопределенности и риска; правильно использовать возможности современных инструментальных средств для анализа, моделирования, оценки информационных процессов предприятий прикладной области в условиях неопределенности и риска.
	ПК-9.3 Владеет навыками принятия эффективных проектных решений на основе приобретенных знаний и умений и их применения в условиях неопределенности и риска; навыками использования современных инструментальных средств при моделировании, оценке и оптимизации информационных процессов предприятий прикладной области; русскоязычной и англоязычной терминологией методов, моделей, инструментария в сфере информационных технологий.

1.2. **Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)»**

Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике и математике в пределах программы средней школы, а также дисциплины младших курсов, такие как

- Криптографические протоколы
- Теория вероятностей и математическая статистика
- Информационные операции и атаки в распределенных информационных системах
- Информационное общество и проблемы прикладной информатики

Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее

- Архитектура сетевой безопасности и управление процессом обеспечения безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Киберпреступность и компьютерная криминалистика» составляет 5 зачетных единиц/180 часов:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		2 курс, 3 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*48*	*48*
Лекции	14	14
Практические занятия	34	34
Лабораторные занятия		
Самостоятельная работа обучающихся	132	132
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет с оценкой	+	+
Экзамен		
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	180\5	180\5

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Основы криминалистики	Понятие, предмет и задачи криминалистики. Система криминалистики. Понятие и научные основы криминалистической идентификации. Криминалистическая диагностика. Предмет, система и задачи трасологии. Научные основы трасологии. Общие положения организации раскрытия и расследования преступлений.	ПК-3, ПК-7, ПК-9
2.	Объекты компьютерной криминалистики	Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.	ПК-3, ПК-7, ПК-9
3.	Аппаратнокомпьютерня и программно-компьютерная экспертизы	Криминалистическая характеристика компьютерных преступлений. Основные группы компьютерных преступлений. Виды компьютерно-технической экспертизы.	ПК-3, ПК-7, ПК-9
4.	Информационно-компьтерная и компьютерно-сетевая экспертизы	Объект, предмет и основные задачи Информационно-компьютерной экспертизы. Основные вопросы, ставящиеся, перед экспертом для проведения информационно -компьютерной экспертизы. Объект, предмет и основные задачи компьютерно-сетевой экспертизы. Компьютерно-сетевая экспертиза как вид компьютерно-технических исследований.	ПК-3, ПК-7, ПК-9

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Основы криминалистики	2	2	4	8	Устный опрос
	Киберпреступления			29	29	Устный опрос
2.	Объекты компьютерной криминалистики	2	4	33	39	Устный опрос
3.	Аппаратнокомпьютерная и программнокомпьютерная экспертизы	4	14	33	51	Устный опрос
4.	Информационнокомпьтерная и компьютерно-сетевая экспертизы	6	14	33	53	Устный опрос
Зачет					2	
	Итого:	14	34	132	180\5	

2.3. Планы теоретических (лекционных) занятий

Тема лекции. Вопросы, отрабатываемые на лекции	Всего часов
Лекция 1. Основы криминалистики Понятие, предмет и задачи криминалистики. Система криминалистики. Понятие и научные основы криминалистической идентификации. Криминалистическая диагностика. Предмет, система и задачи трасологии. Научные основы трасологии. Общие положения организации раскрытия и расследования преступлений	2
Лекция 2 Объекты компьютерной криминалистики. Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.	2
Лекция 3. Аппаратно-компьютерная и программно-компьютерная экспертизы Криминалистическая характеристика компьютерных преступлений. Основные группы компьютерных преступлений. Виды компьютерно-технической экспертизы.	4
Лекция 4. Информационнокомпьтерная и компьютерно-сетевая экспертизы Объект, предмет и основные задачи информационно-компьютерной экспертизы. Основные вопросы, ставящиеся, перед экспертом для проведения информационно -компьютерной экспертизы. Объект, предмет и основные задачи компьютерно-сетевой экспертизы. Компьютерно-сетевая экспертиза как вид компьютерно-технических исследований.	6

2.4. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Всего часов
Практикум 1. Основы криминалистики Классификация криптографических методов	2
Практикум 2. Объекты компьютерной криминалистики Асимметричные криптосистемы.	4
Практикум 3. Аппаратно-компьютерная и программно-компьютерная экспертизы Компьютерно-технические экспертизы: принципы реализации, виды, специфика применения	14
Практикум 4. Информационно-компьтерная и компьютерно-сетевая экспертизы Принципы проведения и специфика информационно-компьютерной экспертизы. Границы использования, решаемые задачи. Принципы проведения и специфика комьютерно-сетевой экспертизы. Границы использования, решаемые задачи.	14

2.5. Планы лабораторных работ – не предусмотрено.

2.7. Задания для самостоятельного изучения

Задания, вопросы, для самостоятельного изучения (задания)	Всего Часов
Основы криминалистики	4
Киберпреступления. Преступления, совершаемые в сфере информационных технологий Виды киберпреступности Особенности киберпреступности Методы обнаружения киберпреступлений. Что грозит за киберпреступления?	29
Объекты компьютерной криминалистики Расследование киберпреступлений. Инструментарий и тренировочные площадки компьютерной криминалистики	33
Аппаратно-компьютерная и программно-компьютерная экспертизы Вопросы, относящиеся к аппаратной компьютерной экспертизе	33
Информационно-компьтерная и компьютерно-сетевая экспертизы Вопросы, относящиеся к информационно-компьютерной экспертизе	33

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

2) для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В.С. Овчинский. — Москва : Норма : ИНФРА-М, 2023. — 528 с. - ISBN 978-5-91768-814-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/2009679

2. Трофимцева, С. Ю. Противодействие киберпреступности: сравнительный анализ международных рекомендаций и норм зарубежного и российского уголовного права : монография / С. Ю. Трофимцева. - Самара : Самарский юридический институт ФСИН России, 2021. - 115 с. Текст: электронный. - URL: https://znanium.com/catalog/product/1871013

3. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — Москва : Издательство Юрайт, 2023. — 417 с. — (Высшее образование) — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520165

4. Бахтеев, Д. В. Криминалистика. Практикум : учебное пособие для вузов / Д. В. Бахтеев. — Москва : Издательство Юрайт, 2023. — 306 с. — (Высшее образование). Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518532

5.2 Перечень дополнительной литературы

1. Особенности противодействия киберпреступности подразделениями уголовного розыска : учебно-метод,ическое пособие для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / А. В. Богданов, И. А. Завьялов, И. И. Ильинский [и др.] ; под ред. Б. П. Михайлова, Е. Н. Хазова. — М. : ЮНИТИ-ДАНА: Закон и право, 2017. — 151 с. - Текст: электронный. - URL: https://znanium.com/catalog/product/1028756

2. Трофимцева, С. Ю. Противодействие киберпреступности: сравнительный анализ международных рекомендаций и норм зарубежного и российского уголовного права : монография / С. Ю. Трофимцева. - Самара : Самарский юридический институт ФСИН России, 2021. - 115 с. - ISBN 978-5-91612-349-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1871013

3. Яблоков, Н. П. Криминалистика : учебник / Н.П. Яблоков. — 2-е изд., перераб. и доп. — Москва : Норма : ИНФРА-М, 2023. — 400 с. - Текст: электронный. - URL: https://znanium.com/catalog/product/1995253

4. Яблоков, Н. П. Криминалистика в вопросах и ответах : учебное пособие / Н. П. Яблоков. - 3-е изд., перераб. - Москва : Норма : ИНФРА-М, 2020. - 288 с. - (Повторительный курс). - Текст: электронный. - URL: https://znanium.com/catalog/product/1088070

5.3. Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.4. Электронные ресурсы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Сетевой анализатор пакетов для анализа вредоносного трафика https://www.wireshark.org/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Федеральный портал «Российское образование www.edu.ru
6. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
7. Сайт Научной электронной библиотеки www.elibrary.ru
8. Электронная библиотека «Знаниум»: https://znanium.com
9. Электронная библиотека «Юрайт»: https://urait.ru
10. Электронно-библиотечная система «Лань»: https://e.lanbook.com/
11. Научная электронная библиотека «Elibrary.ru»: https://www.elibrary.ru/defaultx.asp
12. Фреймворк для криминалистического анализа https://github.com/arxsys/dff

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2.	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	**Критерии оценки**			
	«неудовлетворительн	**«удовлетворительно**	**«хорошо»**	**«отлично»**

	0»	**»**		
ЗНАТЬ				
1	Студент не усвоил следующие знания: правовую и нормативную базу корпоративных информационных систем отраслей; информационную структуру и информационные ресурсы сетей отраслей как объекта защиты;	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания по темам: основные устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ;	Студент способен самостоятельно выделять главные положения в изученном материале. Знает: правовую и нормативную базу корпоративных информационных систем отраслей; информационную структуру и информационные ресурсы сетей отраслей как объекта защиты; основные устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; специальное программное обеспечение по защите информации ПЭВМ;	Студент усвоил основное содержание материала дисциплины :правовую и нормативную базу корпоративных информационных систем отраслей; информационную структуру и информационные ресурсы сетей отраслей как объекта защиты; основные устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; специальное программное обеспечение по защите информации ПЭВМ; основные типы методов, устройств и систем технической разведки;

УМЕТЬ				
2	Студент не умеет создавать простейшие статические webдокуграфическом многооконном режиме, так и в режиме командной строки (консоли); использовать уровни защиты информации; использовать криптографические методы защиты информации;	Студент испытывает затруднения при использовании уровней защиты информации; использовании криптографических методов защиты информации; Не умеет: использовать протоколы взаимной аутентификации объектов сетей; использовать методы организации систем защиты информации ; применять современные системные программные средства, технологии и инструментальные средства;	Студент умеет использовать уровни защиты информации; использовать криптографические методы защиты информации; использовать протоколы взаимной аутентификации объектов сетей; использовать методы организации систем защиты информации ; применять современные системные программные средства, технологии и инструментальные средства;	Студент умеет использовать уровни защиты информации; использовать криптографические методы защиты информации; использовать протоколы взаимной аутентификации объектов сетей; использовать методы организации систем защиты информации ; применять современные системные программные средства, технологии и инструментальные средства; - размещать сценарии PHP на HTML - странице; - использовать графические программы для создания чертежей структуры web - сайта; - использовать графические редакторы для обработки изображений, размещаемых на web -сайте
ВЛАДЕТЬ				
3	Студент не владеет следующими знаниями: DataGridView; навыками работы с межсетевыми экранами и пакетами	Студент владеет DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками	Студент владеет DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками	Студент владеет DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками

	антивирусных программ; навыками самостоятельного проектирования систем защиты информации.	самостоятельного проектирования систем защиты информации.	самостоятельного проектирования систем защиты информации. с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы в системе Windows;	самостоятельного проектирования систем защиты информации. с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы в системе Windows; навыками разработки статических и динамических страниц сети Internet - навыками программирования на языке PHP
	Компетенции или их части не сформированы.	Компетенции или их части сформированы на базовом уровне.	Компетенции или их части сформированы на среднем уровне.	Компетенции или их части сформированы на высоком уровне.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
3	Л	Лекция-беседа, ТСО (мультимедийный проектор, презентации PowerPoint)	14
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	34
	ЛР	Не предусмотрены	
	КР	Устный опрос	
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	132
Итого:			180

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос, защита отчетов по практическим работам, работа на компьютерах в парах, презентация в режиме диалога, работа в парах.

Промежуточная аттестация – зачет с оценкой.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.3. Вопросы к зачету

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты ИБ
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации». Понятие «риска информационной безопасности».
5. Примеры преступлений в сфере информации и информационных технологий.
6. Сущность функционирования системы защиты информации.
7. Защита человека от опасной информации и от неинформированности в области ИБ.
8. Целостность, доступность и конфиденциальность информации.
9. Классификация информации по видам тайны и степеням конфиденциальности.
10. Понятия государственной тайны и конфиденциальной информации.
11. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
12. Цели и задачи защиты информации.
13. Основные понятия в области защиты информации.
14. Элементы процесса менеджмента ИБ.
15. Модель интеграции ИБ в основную деятельность организации.
16. Понятие Политики безопасности.
17. Понятие угрозы безопасности информации
18. Системная классификация угроз безопасности информации
19. Каналы и методы несанкционированного доступа к информации
20. Уязвимости. Методы оценки уязвимости информации
21. Анализ существующих методик определения требований к защите информации
22. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации
23. Виды мер и основные принципы защиты информации
24. Организационная структура системы защиты информации
25. Законодательные акты в области защиты информации
26. Российские и международные стандарты, определяющие требования к защите информации
27. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации
28. Основные механизмы защиты информации.
29. Система защиты информации.
30. Меры защиты информации, реализуемые в автоматизированных (информационных) системах

31. Программные и программно-аппаратные средства защиты информации
32. Инженерная защита и техническая охрана объектов информатизации
33. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим.
34. Принципы построения организационно-распорядительной системы
35. Понятие, предмет и задачи криминалистики
36. Система криминалистики. Понятие и научные основы криминалистической идентификации
37. Криминалистическая диагностика. Предмет, система и задачи трасологии
38. Общие положения оганизации раскрытия и расследования преступлений
39. Криминалистическая характеристика компьютерных преступлений.
40. Основные группы компьютерных преступлений.
41. Виды компьютерно-технической экспертизы
42. Объект, предмет и основные задачи информационно-компьютерной экспертизы.
43. Основные вопросы, ставящиеся, перед экспертом для проведения информационно -компьютерной экспертизы.
44. Объект, предмет и основные задачи компьютерно-сетевой экспертизы.
45. Компьютерно-сетевая экспертиза как вид компьютерно-технических исследований.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-4*	ПК-3, ПК-7, ПК-8

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой