Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.10.2023 17:45:51
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета информационных технологий
/Д. Г. Демидов/
«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы форензики»
Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Безопасность открытых информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2021

Москва 2021 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Основы форензики» следует отнести:

- получение выпускниками знаний о раскрытии преступлений, связанных с компьютерной информацией, об исследовании доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств.

К **основным задачам** освоения дисциплины «Основы форензики» следует отнести:

- знание основ компьютерной криминалистики, правовых норм расследований инцидентов информационной безопасности, алгоритмов расследований инцидентов информационной безопасности;
- умение самостоятельно проводить расследования инцидентов информационной безопасности, проводить компьютерно-техническую экспертизу;
- приобретение опыта поиска цифровых следов в компьютерных системах, фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, документирования противоправных действий злоумышленника.

2. Место дисциплины в структуре ООП.

Дисциплина «Основы форензики» относится к числу профессиональных учебных дисциплин элективной части цикла (Б.1.ДВ) основной образовательной программы (Б.1.ДВ.5).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Организационное и правовое обеспечение информационной безопасности, Безопасность сетей электронных вычислительных машин, Безопасность операционных систем, Защита конфиденциальной информации и персональных данных.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности	**Знать:** • основы компьютерной криминалистики; • правовые нормы расследований инцидентов информационной безопасности; • алгоритмы расследований инцидентов информационной безопасности;

	автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**Уметь:** • самостоятельно проводить расследования инцидентов информационной безопасности; • проводить компьютерно-техническую экспертизу; • документировать противоправные действия злоумышленника. **Владеть:** • методами поиска цифровых следов в компьютерных системах; • методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; • навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 6 семестре.

Структура и содержание дисциплины «Основы форензики» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Понятие информационных преступлений

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

Онлайн-мошенничество. Клевета, оскорбления и экстремистские действия в Сети. Вредоносные программы. Скиминг. Посреднические онлайн-сервисы. Нарушение авторских прав. Фишинг. Киберсквоттинг. Платежи через Интернет.

Тема 2. Криминалистическая характеристика преступлений в сфере компьютерной информации

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

Способы воздействия на информацию при совершении преступлений. Система материальных и идеальных следов компьютерных преступлений. Сведения о предполагаемой личности преступника.

Тема 3. Компьютерно-техническая экспертиза

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

Проблемы назначения эксперта. Проблемы с постановкой вопросов эксперту. Влияние фактора времени на КТЭ. Взаимодействие с пользователем. Стоимость КТЭ.

Тема 4. Совершенствование практики расследования и предупреждения информационных преступлений

Методика расследования информационных преступлений. Корректность и неизменность информации при изъятии. Общие правила изъятия компьютерной техники при обыске. Особенности работы следователя с доказательственной информацией: на ноутбуках; на КПК; на флэш-накопителях; на мобильных телефонах и коммутаторах; на автомобильных видеорегистраторах, цифровых фотоаппаратах. Предупреждение компьютерных преступлений. Особенности предупреждения информационных преступлений в информационно-телекоммуникационной сети Интернет.

Выдвижение следственных версий в зависимости от исходной информации. Программно-техническое обеспечение процесса подготовки и производства следственных действий. Тактика производства отдельных следственных действий.

5. Образовательные технологии.

Методика преподавания дисциплины «Основы форензики» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % аудиторных занятий

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

Образцы билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.
В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-19 Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: •основы компьютерной криминалистики; •правовые нормы расследований инцидентов информационной безопасности; •алгоритмы расследований инцидентов информационной безопасности.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: •основы компьютерной криминалистики; •правовые нормы расследований инцидентов информационной безопасности; •алгоритмы расследований инцидентов информационной безопасности..	Обучающийся демонстрирует неполное соответствие следующих знаний: •основы компьютерной криминалистики; •правовые нормы расследований инцидентов информационной безопасности; •алгоритмы расследований инцидентов информационной безопасности. Допускаются значительные ошибки, проявляется	Обучающийся демонстрирует частичное соответствие следующих знаний: •основы компьютерной криминалистики; •правовые нормы расследований инцидентов информационной безопасности; •алгоритмы расследований инцидентов информационной безопасности, но допускаются	Обучающийся демонстрирует полное соответствие следующих знаний: •основы компьютерной криминалистики; •правовые нормы расследований инцидентов информационной безопасности; •алгоритмы расследований инцидентов информационной безопасности, свободно оперирует приобретенными

		недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	незначительные ошибки, неточности, затруднения при аналитических операциях.	знаниями.
уметь: •самостоятельно проводить расследования инцидентов информационной безопасности; •проводить компьютерно-техническую экспертизу; •документировать противоправные действия злоумышленника.	Обучающийся не умеет или в недостаточной степени умеет •самостоятельно проводить расследования инцидентов информационной безопасности; •проводить компьютерно-техническую экспертизу; •документировать противоправные действия злоумышленника.	Обучающийся демонстрирует неполное соответствие следующих умений: •самостоятельно проводить расследования инцидентов информационной безопасности; •проводить компьютерно-техническую экспертизу; •документировать противоправные действия злоумышленника. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: •самостоятельно проводить расследования инцидентов информационной безопасности; •проводить компьютерно-техническую экспертизу; •документировать противоправные действия злоумышленника. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: •самостоятельно проводить расследования инцидентов информационной безопасности; •проводить компьютерно-техническую экспертизу; •документировать противоправные действия злоумышленника. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: •методами поиска цифровых следов в компьютерных системах; •методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; •навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы.	Обучающийся не владеет или в недостаточной степени владеет •методами поиска цифровых следов в компьютерных системах; •методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; •навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности	Обучающийся владеет •методами поиска цифровых следов в компьютерных системах; •методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; •навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, но допускаются значительные ошибки, проявляется	Обучающийся частично владеет •методами поиска цифровых следов в компьютерных системах; •методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; •навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, навыки освоены, но	Обучающийся в полном объеме владеет •методами поиска цифровых следов в компьютерных системах; •методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; •навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, свободно

	системы.	недостаточность владения	допускаются незначительные ошибки, неточности, затруднения.	применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Рассолов, И. М. Право и Интернет: теоретические проблемы / И. М. Рассолов. — М. : Норма, 2009. — 383 с.

б) дополнительная литература:

1. Вехов, В. Б. Компьютерные преступления: способы совершения и раскрытия / В. Б. Вехов ; под ред. акад. Б. П. Смагоринского. — М. : Право и Закон, 1996.
2. Вехов, В. Б. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.- практич. пособие / В. Б. Вехов, Д. А. Илюшин, В. В. Попова. — 2-е изд. — М. : ЛексЭст, 2004.
3. Войскунский, А. Е. Психологические исследования феномена Интернетаддикции / А. Е. Войскунский // Материалы Второй Российской конференция по экологической психологии. Тезисы (г. Москва, 12—14 апреля 2000 г.). — М. : Экспоцентр — С. 251—253.
4. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : Солон-Пресс, 2002.
5. Гуманитарные исследования в Интернете. — М., 2000.
6. Завидов, Б. Д. Обычное мошенничество и мошенничество в сфере высоких технологий / Б. Д. Завидов. — М., 2002.
7. Иванов, Н. А. Применение специальных познаний при проверке «цифрового алиби» // Информационное право. — 2006. — № 4 (7).
8. Крылов, В. В. Расследование преступлений в сфере информации / В. В. Крылов. — М. : Городец, 1998.
9. Мещеряков, В. А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект / В. А. Мещеряков. — Воронеж, 2001.
10. Митрохина, Е. Информационные технологии, Интернет, интернетзависимость // Наука, политика, предпринимательство. — 2004. — № 1. — С. 83.
11. Михайлов, И. Ю. Методические рекомендации: Носители цифровой информации (обнаружение, изъятие, назначение компьютерно-технической экспертизы) / И. Ю. Михайлов. — Курган : ЭКЦ при УВД Курганской области, 2003.
12. Панарин, И. Технология информационной войны / И. Панарин. — М. : Изд-во «КСП+», 2003.
13. Почепцов, Г. Г. Информационные войны / Г. Г. Почепцов. — М. : Рефл-бук ; К. : Ваклер, 2000. — 576 с.
14. Рабовский, С. В. Социальные аспекты информатизации российского общества / С. В. Рабовский. — М., 2001.
15. Серго, А. Г. Доменные имена / А. Г. Серго. — М. : Бестселлер, 2006.
16. Середа, С. А. Расширительное толкование терминов «вредоносная программа» и «неправомерный доступ» / С. А. Середа, Н. Н. Федотов // Закон. — 2007. — № 7. — С. 191—202.
17. Соловьев, Л. Н. Классификация способов совершения преступлений, связанных с использованием и распространением вредоносных программ для ЭВМ : автореф. дис. … канд. юрид. наук : 12.00.09 / Л. Н. Соловьев. — М., 2003. — 275 с.
18. Федотов, Н. Н. DoS-атаки в Сети. Введение, текущая практика и прогноз // Документальная электросвязь. — 2004. — № 13 [Электронный ресурс] // Доступ : http://www.rtcomm.ru/about/press/pa/? id=429.
19. Федотов, Н. Н. Реликтовое право // Закон и право. — 2007. — № 4. — С. 18—20.
20. Фирсов, Е. П. Расследование изготовления или сбыта поддельных денег или ценных бумаг, кредитных либо расчетных карт и иных платежных документов : монография / Е.

П. Фирсов ; под науч. ред. д-ра юрид. наук, проф. В.И. Комисарова. — М. : Юрлитинформ, 2004.

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

11. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: к.т.н., доцент Н.В. Федоров

Программа утверждена на заседании кафедры “Информационная безопасность” «30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»



к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Основы форензики»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	6 семестр														
1	Тема 1. Понятие информационных преступлений	6	1-2			8	8								
2	Тема 2. Понятие информационных преступлений		3-4			8	8								
3	Тема 3. Криминалистическая характеристика преступлений в сфере компьютерной информации		5-8			16	16								
4	Тема 4. Компьютерно-техническая экспертиза		9-13			20	20								
5	Тема 5. Совершенствование практики расследования и предупреждения информационных преступлений		14-18			20	20								
	Форма аттестации		19-21							.				Э	
	Всего часов по дисциплине во шестом семестре					72	72								
	Всего часов по дисциплине					72	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Основы форензики»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Экзамен

Составители: доц. Федоров Н.В.

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Основы форензики					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать: • основы компьютерной криминалистики; • правовые нормы расследований инцидентов информационной безопасности; • алгоритмы расследований инцидентов информационной безопасности; Уметь: • самостоятельно проводить расследования инцидентов информационной безопасности; • проводить компьютерно-техническую экспертизу; • документировать противоправные действия злоумышленника. Владеть: • методами поиска цифровых следов в компьютерных системах; • методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; • навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы.	самостоятельная работа, лабораторные занятия	экзамен	Базовый уровень: Знать: • основы компьютерной криминалистики; • правовые нормы расследований инцидентов информационной безопасности; • алгоритмы расследований инцидентов информационной безопасности; Уметь: • проводить компьютерно-техническую экспертизу; • документировать противоправные действия злоумышленника. Владеть: • методами поиска цифровых следов в компьютерных системах; • методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах; Повышенный уровень: Уметь: • самостоятельно проводить расследования инцидентов информационной безопасности; Владеть: • навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы.

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

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. **З**начение 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.

Пример билета.

1. Криминалистическая характеристика фишинга.
2. Организационно-технические меры предупреждения информационных преступлений.