


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф., д.т.н., доц.
(должность, уч. степень, звание)
 С.В. Бездатева
(подпись)
«24» июня 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Компьютерная экспертиза»
(Название дисциплины)

Код направления	10.05.05
Наименование направления/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Технологии защиты информации в правоохранительной сфере
Форма обучения	очная

Санкт-Петербург– 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

проф., д.т.н., доц.
должность, уч. степень, звание

«24» июня 2021 г.
подпись, дата



С.В. Бездатева
инициалы, фамилия

Программа одобрена на заседании кафедры № 34

«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34

проф., д.т.н., доц.
должность, уч. степень, звание

«24» июня 2021 г.
подпись, дата



С.В. Бездатева
инициалы, фамилия

Ответственный за ОП 10.05.05(01)

доц., к.т.н., доц.
должность, уч. степень, звание

 24.06.21
подпись, дата

В.А. Мыльников
инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц., к.э.н., доц.
должность, уч. степень, звание

 24.06.21
подпись, дата

Г.С. Армашова-Тельник
инициалы, фамилия

Аннотация

Дисциплина «Компьютерная экспертиза» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» специализация «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

профессиональных компетенций:

ПК-27 «способность готовить научные отчеты по результатам выполненных исследований»,

ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»,

ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»,

Содержание дисциплины охватывает круг вопросов, связанных с решением задачи использования специальных знаний в целях установления фактических данных, способствующих расследованию, раскрытию и предупреждению преступлений, сопряженных с использованием информационных средств и технологий.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью освоения дисциплины является подготовка специалистов, способных квалифицированно и на современном уровне решать задачи использования специальных знаний в целях установления фактических данных, способствующих расследованию, раскрытию и предупреждению преступлений, сопряженных с использованием информационных средств и технологий.

Задачи:

- сформировать знания о свойствах информации как предмета экспертного исследования, видах информации, принципах изъятия и исследования информации;
- изучение системы методов и средств компьютерной экспертизы, а также овладение специальной терминологией;
- изучение основных методов обнаружения и фиксации криминалистически значимой информации, закономерностей слеодообразования в рамках компьютерной экспертизы.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-27 «способность готовить научные отчеты по результатам выполненных исследований»:

знать – правила построения научных отчетов;
 уметь – подбирать информацию для формирования отчетности;
 владеть навыками – формирования отчетов о результатах деятельности;
 иметь опыт деятельности – работы с отчетами по компьютерной экспертизе;

ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»:

знать – состав документации по результатам компьютерной экспертизы;
 уметь – составлять документы по результатам компьютерной экспертизы;
 владеть навыками – учета нормативных и методических документов в области безопасности информации;
 иметь опыт деятельности – формирования документации;

ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»:

знать – методы и технологии компьютерной экспертизы;
 уметь – проводить компьютерную экспертизу;
 владеть навыками – использования специальных информационных технологий для проведения компьютерной экспертизы;
 иметь опыт деятельности – создания отдельных элементов системы безопасности;

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Математические основы обработки информации
- Производственная (эксплуатационная) практика
- Основы информационной безопасности
- Производственная практика

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Научно-исследовательская работа
- Научно-технический семинар
- Производственная преддипломная практика

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№9
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
<i>Из них часов практической подготовки</i>	17	17
<i>Аудиторные занятия, всего час., В том числе</i>	34	34
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	45	45
<i>Самостоятельная работа, всего</i>	29	29
Вид промежуточного контроля: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 9					
Раздел 1. Криминалистическая характеристика преступлений в сфере компьютерной информации	6		4		10
Раздел 2. Методики исследования компьютерной информации при экспертных исследованиях	6		4		9
Раздел 3. Решение экспертных криминалистических задач	5		9		10
Итого в семестре:	17		17		29
Итого:	17	0	17	0	29

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
Раздел 1. Криминалистическая характеристика преступлений в сфере компьютерной информации	<ol style="list-style-type: none"> 1. Классификация компьютерных преступлений. 2. Причины и условия, способствующие совершению компьютерных преступлений. 3. Организационно-технические меры предупреждения компьютерных преступлений. 4. Неправомерный доступ к компьютерной информации. 5. Создание, использование и распространение вредоносных программ для ЭВМ. 6. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
Раздел 2. Методики исследования компьютерной информации при экспертных исследованиях	<ol style="list-style-type: none"> 1. Следообразующие признаки преступной деятельности в сфере телекоммуникации. 2. Осмотр средств вычислительной техники, документов и их носителей. 3. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг сети Интернет. 4. Вопросы, выносимые на разрешение компьютерной экспертизы.
Раздел 3. Решение экспертных криминалистических задач	<ol style="list-style-type: none"> 1. Поиск информации, созданной с помощью прикладных программ. 2. Поиск компьютерной информации по заданным критериям. 3. Поиск информации о действиях пользователя в компьютерной системе. 4. Исследование платежных карт.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего:				

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 9				
1	Классификация экспертных криминалистических задач	1	1	1
2	Осмотр средств вычислительной техники, документов и их носителей	2	2	2
3	Производство обыска при расследовании преступлений в сфере предоставления услуг сети Интернет	2	2	2
4	Классификационные исследования компьютерных систем	2	2	2
5	Диагностические исследования компьютерных систем	2	2	2
6	Поиск информации, созданной с помощью прикладных программ	2	2	3
7	Поиск компьютерной информации по заданным критериям	2	2	3
8	Поиск информации о действиях пользователя в компьютерной системе	2	2	3
9	Исследование платежных карт	2	2	3
Всего:		17	17	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 9, час
1	2	3

Самостоятельная работа, всего	29	29
изучение теоретического материала дисциплины (ТО)	10	10
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	19	19
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.05В 75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	(74)
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с	(8)
Х Я 47	Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.	(9)
	http://e.lanbook.com/books/element.php?pl1_id=3032 Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в
------	-------------------------------------	--------------------------

		библиотеке (кроме электронных экземпляров)
004 М 48	Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с.	(5)
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с.	(10)
	http://e.lanbook.com/books/element.php?pl1_id=4959 Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 с.	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
http://www.intuit.ru/studies/courses/10/10/info	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Задачи; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ПК-27 «способность готовить научные отчеты по результатам выполненных исследований»	
5	Математические основы обработки информации
6	Производственная (эксплуатационная) практика
7	Безопасность систем баз данных
8	Производственная практика
9	Научно-технический семинар
9	Научно-исследовательская работа
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Научно-исследовательская работа
9	Компьютерная экспертиза
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-технический семинар
10	Производственная преддипломная практика
ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»	
4	Основы информационной безопасности
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей

7	Распределенные информационные системы
8	Защита и обработка документов ограниченного доступа
9	Компьютерная экспертиза
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Технологии защищенного документооборота
ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»	
4	Основы информационной безопасности
4	Производственная (технологическая) практика
5	Криптографическая защита информации
5	Информационно-психологическое обеспечение правоохранительной деятельности
6	Криптографическая защита информации
7	Распределенные информационные системы
7	Защита компьютерных сетей
7	Безопасность сетей ЭВМ
8	Защита информации в распределенных информационных системах
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Компьютерная экспертиза
10	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4–балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \leq K \leq 100$	«отлично» «зачтено»	<ul style="list-style-type: none"> - обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.

$70 \leq K \leq 84$	«хорошо» «зачтено»	<ul style="list-style-type: none"> - обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \leq K \leq 69$	«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> - обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$K \leq 54$	«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> - обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	<ol style="list-style-type: none"> 1. Понятие компьютерного преступления. 2. Субъекты компьютерных преступлений. 3. Особенности юридической оценки правонарушений в сфере компьютерной информации. 4. Международная классификация преступлений в сфере высоких технологий. 5. Классификация компьютерных преступлений в соответствии с законодательством России. 6. Преступления в сфере телекоммуникаций. 7. Особенности криминального использования компьютерной техники в экономической сфере и материальном производстве. 8. Неправомерный доступ к компьютерной информации. 9. Создание, использование и распространение вредоносных программ для ЭВМ. 10. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. 11. Контроль над компьютерной преступностью в России. 12. Криминалистическая характеристика преступлений в сфере компьютерной информации. 13. Организация и проведение доследственной проверки сообщения о преступлении в сфере компьютерной информации. 14. Направления расследования преступлений в сфере компьютерной информации. 15. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг сети Интернет.

	16. Осмотр средств вычислительной техники, документов и их носителей. 17. Механизмы слеодообразования в компьютерных системах. 18. Слеодообразующие признаки преступной деятельности в сфере телекоммуникации. 19. Экспертные исследования по расследовании преступлений в сфере компьютерной информации. 20. Вопросы, выносимые на разрешение компьютерной экспертизы. 21. Общие вопросы исследования компьютерной информации. 22. Поиск информации, созданной с помощью прикладных программ. 23. Поиск информации о действиях пользователя. 24. Исследование платежных карт с магнитной полосой. 25. Причины и условия, способствующие совершению компьютерных преступлений. 26. Организационно-технические меры предупреждения компьютерных преступлений.
--	--

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	<p>1. Требования к техническому обеспечению системы защиты <i>аппаратурные и физические</i> управленческие и документарные процедурные и отдельные административные и аппаратурные</p> <p>2. У всех программных закладок имеется общая черта <i>обязательно выполняют операцию записи в память</i> перехватывают прерывания обязательно выполняют операцию чтения из памяти постоянно находятся в оперативной памяти</p>

3. Цель прогресса внедрения и тестирования средств защиты —
гарантировать правильность реализации средств защиты
 выбор мер и средств защиты
 определить уровень расходов на систему защиты
 выявить нарушителя

4. Являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры, клавиатурные шпионы типа
фильтры
 перехватчики
 заместители
 имитаторы

5. «Уполномоченные серверы» фильтруют пакеты на уровне
приложений
 транспортном
 канальном
 физическом

6. ACL-список ассоциируется с каждым
объектом
 типом доступа
 доменом
 процессом

7. Администратор сервера баз данных имеет имя
ingres
 admin
 sysadm
 root

8. Битовые протоколы передачи данных реализуются на
 _____ уровне модели взаимодействия открытых систем
физическом
 сетевом
 транспортном
 канальном

9. Брандмауэры первого поколения представляли собой
маршрутизаторы с фильтрацией пакетов
 «неприступные серверы»
 «уполномоченные серверы»
 хосты с фильтрацией пакетов

10. В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен
доминировать
 быть равен
 быть меньше
 специально оговариваться

	<p>11. В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен <i>быть равен</i> доминировать специально оговариваться быть меньше</p> <p>12. В СУБД Oracle под ролью понимается <i>набор привилегий</i> совокупность процессов группа объектов группа субъектов</p> <p>13. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство <i>доступность</i> восстанавливаемость целостность детерминированность</p> <p>14. Дескриптор защиты в Windows 2000 содержит список <i>пользователей и групп, имеющих доступ к объекту</i> объектов, не доступных пользователям привилегий, назначенных пользователю объектов, доступных пользователю и группе</p> <p>15. Для создания базы данных пользователь должен получить привилегию от <i>администратора сервера баз данных</i> сетевого администратора системного администратора старшего пользователя своей группы</p>
--	---

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	<p>Тема дисциплины Криминалистическая характеристика преступлений в сфере компьютерной информации</p> <ol style="list-style-type: none"> 1. Терминология, объекты и субъекты высоких технологий. 2. Правовая регламентация информационных технологий. 3. Понятие и сущность компьютерной информации. 4. Характеристика преступлений в сфере высоких технологий. 5. Понятие компьютерного преступления. 6. Субъекты компьютерных преступлений. 7. Особенности юридической оценки правонарушений в сфере компьютерной информации. 8. Неправомерный доступ к компьютерной информации. 9. Создание, использование и распространение вредоносных программ для ЭВМ. 10. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

	<p>Тема дисциплины Методики исследования компьютерной информации при экспертных исследованиях</p> <ol style="list-style-type: none"> 1. Расследование преступлений в сфере компьютерной информации. 2. Криминалистическая характеристика преступлений в сфере компьютерной информации. 3. Направления расследования преступлений в сфере компьютерной информации. 4. Назначение компьютерных экспертиз при расследовании преступлений в сфере высоких технологий. 5. Механизмы слеодообразования в компьютерных системах. 6. Слеодообразующие признаки преступной деятельности в сфере телекоммуникации. 7. Объекты компьютерной экспертизы. 8. Вопросы, выносимые на разрешение компьютерной экспертизы. <p>Тема дисциплины Решение экспертных криминалистических задач</p> <ol style="list-style-type: none"> 1. Исследование компьютерной информации. 2. Требования к вопросам, выносимым на компьютерную экспертизу. 3. Последовательность действий по подготовке к поиску компьютерной информации. 4. Поиск компьютерной информации по заданным критериям. 5. Поиск информации, созданной с помощью прикладных программ. 6. Поиск информации о действиях пользователя. 7. Исследование информации, находящейся на магнитной полосе платежных карт. 8. Исследование информации, находящейся на магнитной полосе платежных карт платежных систем Visa и MasterCard.
--	--

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Целью освоения дисциплины является подготовка специалистов, способных квалифицированно и на современном уровне решать задачи использования специальных знаний в целях установления фактических данных, способствующих расследованию, раскрытию и предупреждению преступлений, сопряженных с использованием информационных средств и технологий.

Задачи:

сформировать знания о свойствах информации как предмета экспертного исследования, видах информации, принципах изъятия и исследования информации;
изучение системы методов и средств компьютерно-технической экспертизы, а также овладение специальной терминологией;
изучение основных методов обнаружения и фиксации криминалистически значимой информации, закономерностей слеодообразования в рамках компьютерно-технической экспертизы.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении

фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Криминалистическая характеристика преступлений в сфере компьютерной информации

Раздел 2. Методики исследования компьютерной информации при экспертных исследованиях

Раздел 3. Решение экспертных криминалистических задач

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Задание на лабораторные работы представлены по темам изучаемой дисциплины и представляют собой реализацию изучаемых моделей и алгоритмов:

Раздел 1. Криминалистическая характеристика преступлений в сфере компьютерной информации

Раздел 2. Методики исследования компьютерной информации при экспертных исследованиях

Раздел 3. Решение экспертных криминалистических задач

Структура и форма отчета о лабораторной работе

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;
3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

Требования к оформлению отчета о лабораторной работе

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники...) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой