Министерство образования и науки Российской Федерации
Филиал Федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет»
в г.Тихорецке

Кафедра уголовного права, процесса и криминалистики

УТВЕРЖДАЮ
Проректор по работе с филиалами
ФГБОУ ВО «Кубанский государственный университет»
_____А.А.Евдокимов
«_08_» _____08_____2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.10.02 РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление подготовки 40.03.01 Юриспруденция
Направленность (профиль) Уголовно-правовой
Форма обучения: очная
Квалификация (степень) выпускника: бакалавр

Тихорецк
2018

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 40.03.01 Юриспруденция

Программу составили:
Зав.кафедрой уголовного права, процесса и криминалистики, канд. юрид. наук, доц. М.С. Сирик
Ст. преподаватель кафедры уголовного права, процесса и криминалистики А.В. Терещенко
30 августа 2018 г.

Рабочая программа дисциплины утверждена на заседании кафедры уголовного права, процесса и криминалистики
30 августа 2018 г. протокол № 1
Заведующий кафедрой, канд. юрид. наук, доц. М.С. Сирик

Утверждена на заседании учебно-методической комиссии филиала по УГН «Юриспруденция»
Протокол № 1 30 августа 2018 г.
Председатель УМК филиала по УГН «Юриспруденция», канд. юрид. наук Р.Я. Мамедов
30 августа 2018 г.

Рецензенты:

П.С. Чудов, доцент кафедры правовых дисциплин филиала ФГБОУ ВО КубГУ в г. Армавире, канд. юрид. наук

А.В. Биркин, Зам.начальника отдела ОМВД России по Тихорецкому району Краснодарского края

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1. Цель освоения дисциплины:

– углубить знания студентов по методике расследования преступлений в сфере компьютерной информации.

1.2. Задачи дисциплины:

- усвоение методики расследования преступлений в сфере компьютерной информации;
- ознакомление с разработанными алгоритмами расследования отдельных видов преступлений в сфере компьютерной информации;
- усвоение особенностей тактики проведения отдельных следственных действий при расследовании преступлений в сфере компьютерной информации.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина относится к дисциплинам по выбору вариативной части Блока 1 «Дисциплины (модули)» учебного плана.

Для успешного освоения дисциплины студент должен иметь базовую подготовку по дисциплине «Уголовное право», «Уголовный процесс», «Криминалистика», «Гарантии прав участников уголовного судопроизводства».

Дисциплина «Расследование преступлений в сфере компьютерной информации» является базовой для успешного освоения таких учебных дисциплин, как «Расследование преступлений в сфере экономики», «Расследование терроризма». Изучение дисциплины необходимо также для успешного прохождения и освоения практик, формирующих профессиональные навыки обучающихся, при подготовке к государственной итоговой аттестации.

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

Изучение данной дисциплины направлено на формирование у обучающихся профессиональных компетенций: ПК-10, ПК-13.

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
ПК-10	способность выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения	сущность и содержание процесса выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений	определять оптимальные способы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений; оформлять процессуальные документы	навыками выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений; навыками оценки тех или иных доказательств с точки зрения их относимости, допустимости, достаточности
ПК-13	способность правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации	основы делопроизводства; правила и особенности составления юридических и иных документов	правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации	навыками составления юридических и иных документов, правильного и полного отражения в них результатов профессиональной деятельности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 1 зач.ед. (36 часов), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид учебной работы		Всего часов	Семестры (часы)			
			8			
Контактная работа (всего), в том числе:		**23,2**	**23,2**			
Аудиторные занятия (всего):		**22**	**22**	-	**-**	**-**
Занятия лекционного типа		6	6	-	-	-
Лабораторные занятия		-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)		16	16	-	-	-
Иная контактная работа (всего):		**1,2**	**1,2**			
Контроль самостоятельной работы (КСР)		1	1	-	-	-
Промежуточная аттестация (ИКР)		0,2	0,2	-	-	-
Самостоятельная работа (всего), в том числе:		**12,8**	**12,8**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		6	6	-	-	-
Выполнение индивидуальных заданий (подготовка рефератов, выполнение упражнений и задач)		4,8	4,8	-	-	-
Подготовка к текущему контролю		2	2	-	-	-
Контроль:		**-**	**-**			
Подготовка к зачету		-	-	-	-	-
Общая трудоемкость	**час.**	**36**	**36**	**-**	**-**	**-**
	в том числе контактная работа	**23,2**	**23,2**			
	зач. ед	**1**	**1**			

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 8 семестре (очная форма).

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	Общая характеристика преступлений в сфере компьютерной информации	16,4	2	8		6,4
2	Расследование преступлений в сфере компьютерной информации	18,4	4	8		6,4
	Итого по дисциплине:		*6*	*16*		*12,8*

2.3. Содержание разделов дисциплины

В данном подразделе приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: В – вопросы для устного опроса; Р – реферат; З – упражнения и задачи; Т – тесты.

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Тема 1. Общая характеристика преступлений в сфере компьютерной информации	Понятие и общая характеристика преступлений против отношений в сфере компьютерной информации. Виды преступлений против отношений в сфере компьютерной информации. Неправомерный доступ к компьютерной информации (ст. 272 УК). Понятие компьютерной информации. Законодательное определение крупного ущерба. Квалифицирующие признаки I (ч. 2 ст. 272 УК), II (ч. 3 ст. 272 УК) и III (ч. 4 ст. 272 УК) степеней. Отличие от мошенничества в сфере компьютерной информации (ст. 159$_6$ УК). Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК). Законодательное определение крупного ущерба. Квалифицирующие признаки I (ч. 2 ст. 273 УК) и II (ч. 3 ст. 273 УК) степеней. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК). Законодательное определение крупного ущерба. Квалифицирующие признаки I степени (ч. 2 ст. 274 УК). Международные и зарубежные уголовно-правовые классификации преступлений в сфере высоких технологий. Становление отечественного уголовно-правового и уголовно, процессуального регулирования в сфере высоких технологий и компьютерной информации.	В
2	Тема 2. Расследование преступлений в сфере компьютерной информации	Понятие и сущность специальных знаний сведущих лиц при расследовании преступлений в сфере высоких технологий. Функции специалиста в области информационных средств и технологий, привлеченного к участию в процессуальных действиях. Формы использования специальных знаний в процессе получения доказательственной и ориентирующей ин, формации с применением цифровых данных. Технологии фиксации электронноцифровых объектов на носителях цифровых данных. Назначение и проведение экспертиз при расследовании преступлений в сфере высоких технологий. Судебная компьютерно-техническая экспертиза и ее основные возможности. Возможности комплексной экспертизы при расследовании преступлений в сфере высоких технологий. Современное состояние преступности в сфере компьютерной информации. Особенности квалификации данного вида преступлений. Особенности возбуждения уголовного дела при наличии признаков состава преступлений в сфере компьютерной информации. Предварительная проверка методы и особенности проведения. Предварительные исследования. Основные ситуации первоначального этапа расследования преступлений и типовые следственные версии. Виды и особенности отдельных следственных действий при расследова-	В

№	Наименование раздела	Содержание раздела	Форма текущего контроля
		нии преступлений в сфере компьютерной информации. Современное состояние преступности в сфере мобильных телекоммуникаций. Особенности квалификации данного вида преступлений. Особенности возбуждения уголовного дела при наличии признаков состава преступлений в сфере мобильных телекоммуникаций. Предварительная проверка методы и особенности про, ведения. Предварительные исследования. Основные ситуации первоначального этапа расследования преступлений и типовые следственные версии. Виды и особенности отдельных следственных действий при расследовании преступлений в сфере мобильных телекоммуникаций. Особенности квалификации мошенничества в сфере компьютерной информации. Особенности возбуждения уголовного дела при наличии признаков состава преступлений. Предварительная проверка методы и особенности проведения. Предварительные исследования. Основные ситуации первоначального этапа расследования преступлений и типовые следственные версии. Виды и особенности отдельных следственных действий при расследовании мошенничества с использованием платежных карт и в сфере компьютерной информации.	

2.3.2 Занятия семинарского типа

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	Тема 1. Общая характеристика преступлений в сфере компьютерной информации	1. Понятие и общая характеристика преступлений против отношений в сфере компьютерной информации. 2. Виды преступлений против отношений в сфере компьютерной информации.	Р, З
2	Тема 1. Общая характеристика преступлений в сфере компьютерной информации	1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Понятие компьютерной информации. 3. Законодательное определение крупного ущерба. 4. Квалифицирующие признаки I (ч. 2 ст. 272 УК), II (ч. 3 ст. 272 УК) и III (ч. 4 ст. 272 УК) степеней. 5. Отличие от мошенничества в сфере компьютерной информации (ст. 159$_6$ УК).	Р, З
3	Тема 1. Общая характеристика преступлений в сфере компьютерной информации	1. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК). 2. Законодательное определение крупного ущерба. 3. Квалифицирующие признаки I (ч. 2 ст. 273 УК) и II (ч. 3 ст. 273 УК) степеней.	Р, З
4	Тема 1. Общая характеристика преступлений в сфере компьютерной информации	1. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК). 2. Законодательное определение крупного ущерба.	Р, З, Т

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
		3. Квалифицирующие признаки I степени (ч. 2 ст. 274 УК). 4. Международные и зарубежные уголовно-правовые классификации преступлений в сфере высоких технологий. 5. Становление отечественного уголовно-правового и уголовно, процессуального регулирования в сфере высоких технологий и компьютерной информации.	
5	Тема 2. Методика расследования преступлений экономических преступлений	1. Понятие и сущность специальных знаний сведущих лиц при расследовании преступлений в сфере высоких технологий. 2. Функции специалиста в области информационных средств и технологий, привлеченного к участию в процессуальных действиях. 3. Формы использования специальных знаний в процессе получения доказательственной и ориентирующей ин, формации с применением цифровых данных. 4. Технологии фиксации электронноцифровых объектов на носителях цифровых данных. Назначение и проведение экспертиз при расследовании преступлений в сфере высоких технологий. 5. Судебная компьютерно-техническая экспертиза и ее основные возможности. Возможности комплексной экспертизы при расследовании преступлений в сфере высоких технологий.	Р, З
6	Тема 2. Предупреждение органами внутренних дел преступлений несовершеннолетних	1. Современное состояние преступности в сфере компьютерной информации. 2. Особенности квалификации данного вида преступлений. 3. Особенности возбуждения уголовного дела при наличии признаков состава преступлений в сфере компьютерной информации. 4. Предварительная проверка методы и особенности проведения. Предварительные исследования. 5. Основные ситуации первоначального этапа расследования преступлений и типовые следственные версии. 6. Виды и особенности отдельных следственных действий при расследовании преступлений в сфере компьютерной информации.	Р, З
7	Тема 2. Методика расследования преступлений экономических преступлений	1. Современное состояние преступности в сфере мобильных телекоммуникаций. 2. Особенности квалификации данного вида преступлений. 3. Особенности возбуждения уголовного дела при наличии признаков состава преступлений в сфере мобильных телекоммуникаций. 4. Предварительная проверка методы и особенности про, ведения. Предварительные исследования. 5. Основные ситуации первоначального этапа расследования преступлений и типовые следственные версии. 6. Виды и особенности отдельных следственных действий при расследовании преступлений в сфере мобильных телекоммуникаций.	Р, З

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
8	Тема 2. Методика расследования преступлений экономических преступлений	1. Особенности квалификации мошенничества в сфере компьютерной информации. 2. Особенности возбуждения уголовного дела при наличии признаков состава преступлений. 3. Предварительная проверка методы и особенности проведения. Предварительные исследования. 4. Основные ситуации первоначального этапа расследования преступлений и типовые следственные версии. 5. Виды и особенности отдельных следственных действий при расследовании мошенничества с использованием платежных карт и в сфере компьютерной информации.	Р, З, Т

2.3.3 Лабораторные занятия

Лабораторные занятия не предусмотрены.

2.3.4 Примерная тематика курсовых работ

Курсовые работы не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Проработка учебного (теоретического) материала	Самостоятельная работа студентов: методические рекомендации для бакалавров направления подготовки 40.03.01 Юриспруденция, утвержденные кафедрой уголовного права, процесса и криминалистики (протокол №1 от 30.08.2018 г.)
2	Подготовка к текущему контролю	
3	Подготовка рефератов	Письменные работы студентов: методические рекомендации для бакалавров направления подготовки 40.03.01 Юриспруденция, утвержденные кафедрой уголовного права, процесса и криминалистики (протокол №1 от 30.08.2018 г.)
4	Выполнение упражнений и задач	

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме;

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме;

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения дисциплины занятия лекционного типа и занятия семинарского типа являются ведущими формами обучения в рамках лекционно-семинарской образовательной системы.

В учебном процессе используются следующие образовательные технологии:

– технология проблемного обучения: последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешая которые студенты активно усваивают знания;

– технология развивающего обучения: ориентация учебного процесса на потенциальные возможности человека и их реализацию;

– технология дифференцированного обучения: усвоение программного материала на различных планируемых уровнях, но не ниже обязательного;

– технология активного (контекстного) обучения: моделирование предметного и социального содержания будущей профессиональной деятельности.

Также при освоении дисциплины в учебном процессе используются активные формы проведения занятий.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств по дисциплине оформлен как отдельное приложение к рабочей программе.

Примерные вопросы для устного опроса

Тема 1. Общая характеристика преступлений в сфере компьютерной информации

1. Дайте понятие компьютерной информации?
2. Типичные следственные ситуации и версии первоначального этапа расследования преступлений в сфере компьютерной информации.
3. Обстоятельства, подлежащие установлению и доказыванию по делам о преступления в сфере компьютерной информации.
4. Особенности организации и проведения допроса свидетеля, потерпевшего по делам о преступления в сфере компьютерной информации.
5. Особенности организации и производства обыска по делам о преступлениях в сфере компьютерной информации.
6. Взаимодействие следователя с оперативными подразделениями на первоначальном этапе расследования преступлений в сфере компьютерной информации.
7. Назовите родовой и видовой объекты преступлений в сфере компьютерной информации?
8. Назовите компьютерные преступления, относящиеся к материальным составам преступлений?
9. Назовите компьютерные преступления, относящиеся к формальным составам преступлений?
10. В чем заключается объективная сторона неправомерного доступа к компьютерной информации?
11. В чем отличие неправомерного доступа к компьютерной информации от нарушения авторских и смежных прав?
12. В чем отличие неправомерного доступа к компьютерной информации от хищения?
13. Назовите бланкетную основу преступлений в сфере компьютерной информации?
14. Что понимается под преступлениями в сфере компьютерной информации?
15. Дайте характеристику неправомерного доступа к компьютерной информации?
16. С какого момента создание вредоносных компьютерных программ считается оконченным преступлением?
17. Является ли компьютерная программа разновидностью компьютерной информации?
18. Какова субъективная сторона нарушения правил эксплуатации средств хранения компьютерной информации?
19. Назовите виды правил, которые могут быть нарушены при эксплуатации ЭВМ?
20. Что понимается под «вредоносной компьютерной программой»?
21. Понятие сферы высоких технологий и кибернетического пространства как среды совершения преступлений.

22. Регулирование общественных отношений в киберпространстве зарубежный опыт и отечественное законодательство.
23. Преступления в сфере высоких технологий.
24. Понятие особенности история развития и современное состояние.

Примерные темы рефератов

Тема 1. Общая характеристика преступлений в сфере компьютерной информации

1. Понятие преступления в сфере компьютерной информации.
2. Развитие отечественного законодательства в сфере борьбы с преступлениями в сфере компьютерной информации.
3. Понятие и общая характеристика преступлений в сфере компьютерной информации.
4. Виды преступлений против отношений в сфере компьютерной информации.
5. Общая характеристика компьютерных преступлений.
6. Общая характеристика преступлений в сфере компьютерной информации
7. Способ преступления в сфере компьютерной информации как главный элемент криминалистической характеристики.
8. Взаимосвязи и взаимозависимости между элементами криминалистической характеристики.
9. Преступления в сфере компьютерной информации.
10. Отграничение компьютерных преступлений от смежных видов преступлений.
11. Особенности квалификации преступлений в сфере компьютерной информации.
12. Классификация способ совершения компьютерных преступлений.

Примерные упражнения и задачи

Тема 1. Общая характеристика преступлений в сфере компьютерной информации

1. В целях уклонения от уплаты налогов владелец магазина Карпов приобрел у программиста Петрова специальную программу и техническое устройство для внесения изменений в фискальную память контрольно-кассовых машин, позволявших оставлять до 60% кассовых операций без учета со стороны налоговых органов. Использование указанных средств позволило Карпову сэкономить в течение года 160 тыс. рублей.

Квалифицируйте действия указанных лиц.

2. Уволенный из военного института Боков сконструировал прибор – сканер, с помощью которого перехватывал идентификационные коды мобильных телефонов легальных пользователей и, вводя их в память своего устройства, осуществлял звонки, счета на оплату которых приходили законным абонентам. Общая сумма в счетах пользователям сотовых телефонов составила 85 тыс. 320 рублей.

В ходе предварительного расследования было установлено, что идентификационный код, перехватываемый боковым в виде радиосигнала и воспринимаемый ЭВМ, находящейся в компании сотовой связи, является компьютерной информацией.

Решите вопрос об ответственности Бокова.

3. Шевцов и Трусов, продолжительное время работая на одном предприятии - ООО "Виктория", вступили в сговор, направленный на хищение ликероводочной продукции. Они обговорили условия, по которым Шевцов создает на фирме условия для получения продукции без предоплаты, а Трусов обеспечивает вывоз и сбыт.

Будучи главным специалистом службы сбыта и маркетинга и зная порядок ввода информации в локальную сеть ЭВМ для последующего получения продукции предприятия с отсрочкой платежа, Шевцов с помощью компьютера проник в локально-вычислительную сеть ЭВМ ООО "Виктория", где, уничтожив в списке клиентов фирмы запись "300" - номер договора с ЗАО "Лотос", ввел в указанный реестр заведомо ложную информацию о фирме "Победа", что послужило основанием для отгрузки последней ликероводочной продукции на сумму 300 тыс. рублей.

Трусов подыскал для исполнения роли экспедитора своего знакомого Котова, а для сбыта похищенного - Стасова, о чем уведомил Шевцова, который на имеющемся у него типовом бланке оформил доверенность от фирмы "Победа" на получение 200 ящиков ликероводочной продукции на имя экспедитора Котова и поставил на нее оттиск печати фирмы "Победа".

Шевцов ввел информацию о фирме "Победа" в локально-вычислительную сеть фирмы "Виктория". На следующий день Котов, используя доверенность фирмы "Победа", вывез со склада ООО "Вик-

тория" 4 тыс. бутылок водки "Столичная" на суммы 300 тыс. рублей. Трусов реализовал водку за наличный расчет Стасову, полученные деньги поделил со Швецовым.

Дайте юридическую оценку действиям указанных лиц.

4. Инженер-программист телефонного завода Лебедев, желая подключиться к сети Интернет за казенный счет, скопировал у своего знакомого Н. программу типа "троянский конь", имитирующую нормальную работу ЭВМ и одновременно негласно для пользователя предоставляющую полный доступ к компьютеру. Эту программу Лебедев направил в виде текстового документа на электронный адрес Н-ского РУФПС.

Эта программа позволила Лебедеву зайти на жесткий диск компьютера РУФПС и скопировать два закодированных файла с паролями доступа к "Всемирной паутине".

Имевшиеся на компьютере Лебедева файлы доступа были заменены им на скопированные с ЭВМ РУФПС. Используя специальную компьютерную программу, Лебедев раскодировал пароль подключения к сети Интернет Н-ского РУФПС с целью его дальнейшего использования, то есть подключения к сети Интернет за счет РУФПС.

Лебедев, достоверно зная имя и пароль РУФПС, в течение полугода систематически подключался к сети Интернет за счет РУФПС, чем причинил данной организации материальный ущерб на сумму 18 тыс.300 руб.

Дайте юридическую оценку действиям Лебедева.

5. Программист Пылаев "из интереса" создал новый компьютерный вирус и записал его на дискету с легальной программой, которую передал своему знакомому Мостову. Результатом действий вируса явилось то, что компьютер Мостова перестал работать в операционной среде Windows. После тестирования ЭВМ антивирусным пакетом вирус был уничтожен.

Дайте юридическую оценку действиям Пылаев.

6. Курочкин, подобрав пароль, вошел через глобальную сеть в защищенный раздел сервера Президента Российской Федерации и скопировал интересующую его информацию. Указанные данные относились к государственной тайне.

Дайте юридическую оценку действиям Курочкина.

7. Оператор ПЭВМ Моргулина "из любопытства" попыталась проникнуть в базу данных системы ведения реестра акционеров ОАО "Техполис", к которой по службе не имела доступа. Результатом ее неквалифицированных действий стало уничтожение dbf-файлов, содержащих данные о количестве акций, принадлежащих каждому конкретному акционеру, и их почтовые адреса.

Варианты: а) Моргулина по службе не имела права доступа к ЭВМ, на которой находилась система ведения реестра акционеров; б) Моргулина совершила указанные действия за вознаграждение по поручению одного из акционеров, желавшего получить домашние адреса акционеров — физических лиц с целью скупить у них акции.

Дайте юридическую оценку действиям Моргулина.

8. Дынина, сотрудник расчетно-кассового отдела банка, привела на работу своего малолетнего сына, который, балуясь, выключил компьютер-сервер, что привело к остановке работы РКО на два часа, в течение которых банк не мог производить операции по счетам клиентов, поэтому на один день было задержано исполнение всех платежных поручений.

Дайте юридическую оценку действиям Дынина.

9. На сборочном конвейере одного из автомобильных заводов России программист Дучин "в шутку" ввел в компьютерную программу паузу при. передаче на конвейер определенного числа деталей. При срабатывании логической бомбы ЭВМ зависала и конвейер останавливался. "Шутка", пока ее не выявили, обходилась в 200 невыпущенных автомобилей в смену.

Дайте юридическую оценку действиям Дучина.

10. Программист Пылаев "из интереса" создал новый компьютерный вирус и записал его на дискету с легальной программой, которую передал своему знакомому Мостову. Результатом действий вируса явилось то, что компьютер Мостова перестал работать в операционной среде Windows. После тестирования ЭВМ антивирусным пакетом вирус был уничтожен.

Варианты: а) Пылаев, проверив действие вируса на своем компьютере, уничтожил его; б) Мостов, догадавшись, что вирус был на дискете Пылаева, передал ее Горбову, с которым имел неприязненные отношения, в пользование, чтобы нарушить работу его ЭВМ.

Дайте юридическую оценку действиям Пылаева.

11. Компания "Браво" по производству и распространению своих компьютерных программ разработала программу для ЭВМ "Defender", одной из особенностей которой было то, что при установке ее

на компьютер она определяла наличие на диске продукции компании "Браво". Если эта продукция была приобретена с нарушением установленных правил (нелегальное копирование), "Defender", определив это, уничтожал такие программы, а также иные системные и программные файлы на такой ЭВМ.

Вариант: "Defender" уничтожал только незаконно скопированную продукцию компании "Браво".

Дайте юридическую оценку действиям компании "Браво".

12. Для разрешения спора они решили создать по компьютерному вирусу, записать его на ЭВМ противника посредством электронной сети и уничтожить вирус противника. В результате этой "дуэли" компьютерная сеть фирмы оказалась заражена одним из вирусов, и руководству "Беркута" пришлось оплатить работу сотрудников специализированной компании по уничтожению вируса и устранению последствий заражения.

Дайте юридическую оценку действиям руководства "Беркута".

13. Челюскин, обнаружив, что во время работы в глобальной сети к нему подключился хакер (компьютерный взломщик), записал на ЭВМ последнего компьютерную программу и активировал ее. Эта программа, разработанная Челюскиным специально для борьбы с компьютерными взломщиками, будучи активированной, не позволила ЭВМ хакера связываться с глобальной сетью.

Дайте юридическую оценку действиям Челюскина.

14. Оператор ПЭВМ адресного бюро Баранова в нарушение правил эксплуатации, не выполнив действий по выходу из программы, выключила компьютер-сервер, что привело к остановке производственного процесса в сети ЭВМ на 2 часа.

Вариант: действия Барановой привели к уничтожению части данных о гражданах, которые вводились в ЭВМ, но еще не были сохранены.

Дайте юридическую оценку действиям Барановой .

15. Орешкин, программист областного статистического управления, по невнимательности переформатировал жесткий диск ЭВМ, содержащий ценную информацию и легальное программное обеспечение (Window 95, Word for Windows, Excel, Power point). Информацию и программы восстановить не удалось.

Дайте юридическую оценку действиям Орешкина.

16. Системный администратор Шарапова в нарушение должностной инструкции уничтожила файловые архивы на дискетах, которые содержали информацию о котировках на валютном рынке и рынке векселей и государственных ценных бумаг.

Дайте юридическую оценку действиям Шарапова.

17. Терещенко записал у своего друга Санникова с его домашнего компьютера игру для ЭВМ. Игра относилась к программам, для которых разрешено свободное копирование. При ее установке на рабочий компьютер автоматически записался компьютерный вирус, о существовании которого на домашней ЭВМ Санников не подозревал. В связи с тем, что ЭВМ Терещенко входила в локальную сеть фирмы, все компьютеры оказались зараженными вирусом. Уничтожение вируса и проверка работы сети заняли 5 часов.

Вариант: в процессе уничтожения вируса выяснилось, что им была повреждена часть информации, которая относилась к коммерческой тайне фирмы.

Дайте юридическую оценку действиям указанных лиц.

Примерные тесты

Тема 1. Общая характеристика преступлений в сфере компьютерной информации

1. Информация это -

а) сведения, поступающие от СМИ;

б) только документированные сведения о лицах, предметах, фактах, событиях;

в)·сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

г) только сведения, содержащиеся в электронных базах данных.

2. Информация

а) не исчезает при потреблении;

б) становится доступной, если она содержится на материальном носителе;

в) подвергается только "моральному износу";

г) характеризуется всеми перечисленными свойствами.

3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется

а) достоверной;

б) конфиденциальной;

в) документированной;

г) коммерческой тайной.

4. Формы защиты интеллектуальной собственности -

а) авторское, патентное право и коммерческая тайна;

б) интеллектуальное право и смежные права;

в) коммерческая и государственная тайна.

г) гражданское и административное право.

5. По принадлежности информационные ресурсы подразделяются на

а) государственные, коммерческие и личные;

б) государственные, не государственные и информацию о гражданах;

в) информацию юридических и физических лиц;

г) официальные, гражданские и коммерческие.

6. К негосударственным относятся информационные ресурсы

а) созданные, приобретенные за счет негосударственных учреждений и организаций;

б) созданные, приобретенные за счет негосударственных предприятий и физических лиц;

в) полученные в результате дарения юридическими или физическими лицами.

8. По доступности информация классифицируется на

а) открытую информацию и государственную тайну;

б) конфиденциальную информацию и информацию свободного доступа;

в) информацию с ограниченным доступом и общедоступную информацию;

г) виды информации, указанные в остальных пунктах.

9. К конфиденциальной информации не относится

а) коммерческая тайна;

б) персональные данные о гражданах;

в) государственная тайна;

г) "ноу-хау".

10. Интеллектуальная собственность включает права, относящиеся к

а) литературным, художественным и научным произведениям, изобретениям и открытиям;

б) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам;

в) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям;

г) всему, указанному в остальных пунктах.

11. Конфиденциальная информация это

а) сведения, составляющие государственную тайну;

б) сведения о состоянии здоровья высших должностных лиц;

в) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ;

г) данные о состоянии преступности в стране.

12. Какая информация подлежит защите?

а) информация, циркулирующая в системах и сетях связи

б) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

в) только информация, составляющая государственные информационные ресурсы;

г) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

13. Классификация и виды информационных ресурсов определены

а) Законом "Об информации, информатизации и защите информации";

б) Гражданским кодексом;

в) Конституцией;

г) всеми документами, перечисленными в остальных пунктах.

14. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?

а) да;
б) нет;
в) только авторское и патентное;
г) только КТ.

15. «Ноу-хау» это -

а) незащищенные новшества;
б) защищенные новшества;
в) общеизвестные новые технологии;
г) опубликованные технические и технологические новинки.

16. К информации ограниченного доступа не относится

а) государственная тайна;
б) размер золотого запаса страны;
в) персональные данные;
г) коммерческая тайна.

17. При расследовании преступлений в сфере компьютерной информации подлежат выявлению следующие обстоятельства

а) способ совершения преступлений;
б) характер и размер причиненного вреда;
в) кто имеет доступ к информации, содержащейся в ЭВМ;
г) все ответы правильные.

18. Под информационной безопасностью понимается…

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;

б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;

в) нет правильного ответа.

19. Защита информации – это..

а) комплекс мероприятий, направленных на обеспечение информационной безопасности;
б) процесс разработки структуры базы данных в соответствии с требованиями пользователей;
в) небольшая программа для выполнения определенной задачи.

20. От чего зависит информационная безопасность?

а) от компьютеров;
б) от поддерживающей инфраструктуры;
в) от информации.

21. Основные составляющие информационной безопасности:

а) целостность;
б) достоверность;
в) конфиденциальность;
г) все ответы правильные.

22. Целостность – это..

а) целостность информации;
б) непротиворечивость информации;
в) защищенность от разрушения;
г) все ответы правильные.

23. Конфиденциальность – это..

а) защита от несанкционированного доступа к информации;

б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов;

в) описание процедур.

24. Для чего создаются информационные системы?

а) получения определенных информационных услуг;
б) обработки информации;
в) все ответы правильные.

25. Целостность можно подразделить:

а) статическую;
б) динамичную;
в) структурную.

26. Где применяются средства контроля динамической целостности?

а) анализе потока финансовых сообщений;
б) обработке данных;
в) при выявлении кражи, дублирования отдельных сообщений.

27. Какие трудности возникают в информационных системах при конфиденциальности?

а) сведения о технических каналах утечки информации являются закрытыми;
б) на пути пользовательской криптографии стоят многочисленные технические проблемы;
в) все ответы правильные.

28. Угроза – это…

а) потенциальная возможность определенным образом нарушить информационную безопасность;
б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;
в) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

29. Какие существуют грани вредоносного П.О.?

а) вредоносная функция;
б) внешнее представление;
в) способ распространения;
в) все ответы правильные.

30. По механизму распространения П.О. различают:

а) вирусы;
б) черви;
в) все ответы правильные.

31. Вирус – это…

а) код обладающий способностью к распространению путем внедрения в другие программы;
б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов;
в) небольшая программа для выполнения определенной задачи.

32. Черви – это…

а) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения;
б) код обладающий способностью к распространению путем внедрения в другие программы;
в) программа действий над объектом или его свойствами.

33. Конфиденциальную информацию можно разделить:

а) предметную;
б) служебную;
в) глобальную.

34. СЗИ (система защиты информации) делится:

а) ресурсы автоматизированных систем;
б) организационно-правовое обеспечение;
в) человеческий компонент;
в) все ответы правильные.

35. Правовое обеспечение безопасности информации – это…

а) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации;
б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;
в) нет правильного ответа.

36. Правовое обеспечение безопасности информации делится:

а) международно-правовые нормы;
б) национально-правовые нормы;
в) все ответы правильные.

37. Информацию с ограниченным доступом делят:

а) государственную тайну;

б) конфиденциальную информацию;
в) достоверную информацию.

38. Вредоносная программа - это…

а) программа, специально разработанная для нарушения нормального функционирования систем;
б) упорядочение абстракций, расположение их по уровням;
в) процесс разделения элементов абстракции, которые образуют ее структуру и поведение.

39. К организационно - административному обеспечению информации относится:

а) взаимоотношения исполнителей;
б) подбор персонала;
в) регламентация производственной деятельности;
в) все ответы правильные.

40. Что относится к организационным мероприятиям:

а) хранение документов;
б) проведение тестирования средств защиты информации;
в) пропускной режим.

41. Программные средства – это…

а) специальные программы и системы защиты информации в информационных системах различного назначения;

б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла;

в) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними.

42. Криптографические средства – это…

а) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования;

б) специальные программы и системы защиты информации в информационных системах различного назначения;

в) механизм, позволяющий получить новый класс на основе существующего.

43. Виды компьютерной информации –

а) общего пользования (общедоступная);
б) охраняемая законом (конфиденциальная);
в) все ответы правильные.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Вопросы для подготовки к зачету

1. Понятие информации.
2. Нормативно закрепленное понятие «информации» в законах РФ.
3. Отличие информации, компьютерной информации, правовой информации.
4. Компьютерные технологии: понятие, значение, сущность.
5. Уголовный кодекс и преступления в сфере компьютерной информации.
6. Объект и объективная сторона.
7. Субъект и субъективная сторона.
8. Квалификационные признаки.
9. Понятие, содержание и основные элементы криминалистической характеристики преступлений в сфере компьютерной информации.
10. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.
11. Личностная характеристика преступника, совершающего компьютерные преступления.
12. Особенности обстановки совершения компьютерных преступлений.
13. Понятие способа совершения компьютерного преступления.
14. Классификация способов совершения компьютерных преступлений.
15. Понятие и классификация следов компьютерных преступлений.

16. Регистрационные файлы операционных систем и регистрационные файлы СУБД как доказательства по делу.

17. Особенности возбуждения уголовного дело при расследовании преступлений в сфере компьютерной информации.

18. Типичные следственные ситуации.

19. Особенности выдвижения и проверки следственных версий.

20. Осмотр места происшествия.

21. Осмотр средства электронно-вычислительной техники.

22. Осмотр машинного носителя информации.

23. Осмотр документа на машинном носителе.

24. Осмотр машинограммы.

25. Изъятие средств электронно-вычислительной техники и компьютерной информации как элемент отдельных следственных действий.

26. Обыск и выемка.

27. Криминалистическое исследование операционных систем и СУБД.

28. Специалист согласно УПК (Процессуальные права и обязанности).

29. Подготовка к проведению следственного действия (например осмотра места происшестия).

30. Требования, предъявляемые к специалисту.

31. Перечень следственный действий проводимых с помощью специалиста.

32. Ограничения при использовании помощи специалиста.

33. Автороведческая экспертиза.

34. Компьютерно-техническая экспертиза.

35. Классификация компьютерно-технических экспертиз.

36. Компьютерно-сетевая экспертиза.

37. Комплексная компьютерно-техническая и технико-криминалистическая экспертиза документов, изготовленных на матричных игольчатых принтерах.

38. Специальные структуры в правоохранительных органах в борьбе с преступлениями в сфере компьютерной информации.

39. Специализированное программное обеспечения для предупреждения и выявления преступлений данной категории.

40. Сущность фиксации следовой информации по делам о компьютерных преступлениях.

41. Особенности фиксации следовой информации о попытках зондирования компьютерных систем или ведения радиоэлектронной разведки.

42. Особенности фиксации следовой информации о действии вредоносных программ в ходе осмотра компьютерных систем и их сете.

43. Особенности фиксации следовой информации при проведении аудита компьютерных систем в ходе осмотра компьютерных систем и их сетей.

Критерии оценивания ответа на зачете

Студенты обязаны сдать зачет в соответствии с расписанием и учебным планом. Зачет по дисциплине преследует цель оценить работу студента за курс, получение теоретических знаний, их прочность, развитие творческого мышления, приобретение навыков самостоятельной работы, умение применять полученные знания для решения практических задач.

Зачет - форма промежуточной аттестации, в результате которого обучающий получает оценку в двухбалльной шкале («зачтено», «не зачтено»).

Оценка «зачтено» ставится студенту, который прочно усвоил предусмотренный программный материал; правильно, аргументировано ответил на все вопросы, с приведением примеров; показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов; без ошибок выполнил практическое задание. Обязательным условием выставленной оценки является правильная речь в быстром или умеренном темпе. Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельной и контрольной работы, систематическая активная работа на семинарских (практических) занятиях.

Оценка «не зачтено» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Нормативные правовые акты и акты судебного толкования:

1 Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

2 Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

3 Уголовно-процессуальный кодекс Российской Федерации (18.12.2001 N 174-ФЗ) (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

4 Об оперативно-розыскной деятельности федеральный закон РФ № 144–ФЗ от 12 августа 1995 г. (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

5 О государственной судебно-экспертной деятельности в Российской Федерации: ФЗ РФ от 31 мая 2001 г. № 73-ФЗ (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

6 О Следственном Комитете РФ: ФЗ РФ от 28 декабря 2010 г. № 403-ФЗ (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

7 Об информации, информационных технологиях и о защите информации от 27 июля 2006 г. N 149-ФЗ (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

8 О связи: Федеральный закон РФ от 7 июля 2003 №58-ФЗ (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

9 О медицинском освидетельствовании подозреваемых или обвиняемых в совершении преступлений: Постановление Правительства РФ от 14 января 2011 г. № 3 (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

10 Инструкция об организации информационного обеспечения сотрудничества по линии Интерпола: утверждена приказом МВД РФ от 06 октября 2006 г. № 786 (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

11 О государственной тайне: Федеральный закон от 21июля 1993 г. №5485-1 (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

12 Инструкция о порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд: утв. приказом МО России, ФСБ России, ФСИН России, МВД России, ФСО России, ФТС России, СВР России от 17 апр. 2007 г. №

368/185/164/481/32/184/97/147 (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

13 Об утверждении Инструкции по организации взаимодействия подразделений и служб внутренних дел в расследовании и раскрытии преступлений (с изменениями от 13 февраля 1997 г., 18 января 1999 г.) Приказ МВД РФ от 20 июня 1996 г. № 334 (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

14 Об утверждении Инструкции о порядке приема, регистрации и разрешения в органах внутренних дел РФ заявлений, сообщений и иной информации о происшествиях: Приказ Министра внутренних дел РФ от 4 мая 2010 г. № 333 (в действующей редакции) // Информационно-правовая система «Гарант» (http://www.garant.ru/)

5.2 Основная литература:

1 Особенности противодействия киберпреступности подразделениями уголовного розыска : учебно-методическое пособие / под ред. П.Б. Михайлова, Е.Н. Хазова. - М. : Юнити-Дана : Закон и право, 2016. - 151 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=439600

2 Филиппов, А. Г. Криминалистика. Полный курс : учебник для бакалавров / А. Г. Филиппов ; под общ. ред. А. Г. Филиппова. — 5-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 855 с. — Режим доступа : www.biblio-online.ru/book/8AEB9B56-36E4-4B56-A204-39B340D25AFA

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечной системе «Юрайт», «Университетская библиотека онлайн».

5.3 Дополнительная литература:

1 Безлепкин, Б.Т. Краткое пособие для следователя и дознавателя / Б.Т. Безлепкин. - 2-е изд., перераб. и доп. - Москва : Проспект, 2017. - 287 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=471811

2 Егоров, Н. Н. Криминалистика в 2 ч. Часть 1 : учебник и практикум для бакалавриата и магистратуры / Н. Н. Егоров, Е. П. Ищенко. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 362 с. — Режим доступа : www.biblio-online.ru/book/FB23C877-60DB-4C3A-8CD5-9FBB4E0339CC

3 Егоров, Н. Н. Криминалистика в 2 ч. Часть 2 : учебник и практикум для бакалавриата и магистратуры / Н. Н. Егоров, Е. П. Ищенко. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 184 с. — Режим доступа : www.biblio-online.ru/book/4BCE9F2D-2C2E-48ED-A823-468C4D4484BC

4 Использование специальных знаний при расследовании преступлений: Учебное пособие / Алехин Д.В.; Под ред. Бастрыкина А.И. - М.:ЮНИТИ-ДАНА, 2016. - 255 с. – Режим доступа: http://znanium.com/catalog/product/560534

5 Криминалистика : учебник для бакалавриата и магистратуры / И. В. Александров [и др.] ; под ред. И. В. Александрова. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 376 с. — Режим доступа : www.biblio-online.ru/book/9598AF55-B0CE-4361-9F9F-D11EDBC0C16D

6 Криминалистика [Текст] : учебное пособие к использованию в образовательных учреждениях, реализующих основные образовательные программы бакалавриата по направлению подготовки "Юриспруденция", по специальностям "Правоохранительная деятельность", "Правовое обеспечение национальной безопасности" / Р. И. Гадельшин, В. К. Кузнецов. - 2-е изд., стер. - Москва : КНОРУС, 2016. - 220 с. (5 экз.)

7 Криминалистика. Практикум : учебное пособие для академического бакалавриата / А. Г. Филиппов [и др.] ; под ред. А. Г. Филиппова, В. В. Агафонова. — М. : Издательство Юрайт, 2017. — 360 с. — Режим доступа : www.biblio-online.ru/book/4B62AF3A-7754-4724-8660-AB3F14A160E3

8 Криминалистика. Сборник задач и заданий [Текст] : учебное пособие / [О. Я. Баев и др.] ; под ред. О. Я. Баева. - Москва : Проспект, 2015. - 271 с. (4 экз.)

9 Криминалистическая методика для дознавателей : учебник для вузов / А. Г. Филиппов [и др.] ; под общ. ред. А. Г. Филиппова. — М. : Издательство Юрайт, 2017. — 414 с. — Режим доступа : www.biblio-online.ru/book/2E9024CC-A677-44D4-B59D-62B83EC1BF73

10 Кульков, В. В. Уголовный процесс. Методика предварительного следствия и дознания : учебное пособие для вузов / В. В. Кульков, П. В. Ракчеева ; под ред. В. В. Кулькова. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 311 с. — (Серия : Специалист). — ISBN 978-5-534-05990-8. — Режим доступа : www.biblio-online.ru/book/F70305C1-BCB9-49ED-A3E7-D965420F9CA3

11 Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В. С. Овчинский. — М. : Норма, 2017. — 528 с. – Режим доступа: http://znanium.com/catalog/product/771246

12 Преступления против общественной безопасности и общественного порядка : учебное пособие для бакалавриата и магистратуры / А. В. Наумов [и др.] ; отв. ред. А. В. Наумов, А. Г. Кибальник. — М. : Издательство Юрайт, 2017. — 141 с. — Режим доступа : www.biblio-online.ru/book/ADEC603A-04D4-4BB5-950E-348AA337F3F6

13 Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации : монография / В.Г. Степанов-Егиянц. - М. : Статут, 2016. - 190 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=452481

14 Уголовное право России. Особенная часть в 2 т. Том 1 : учебник для академического бакалавриата / О. С. Капинус [и др.] ; отв. ред. О. С. Капинус. — М. : Издательство Юрайт, 2018. — 437 с. — Режим доступа : www.biblio-online.ru/book/C580BE48-1A50-46AE-B67C-6A670FA58508

15 Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учеб. пособие / Е.А. Русскевич. — М. : ИНФРА-М, 2018. — 115 с. – Режим доступа: http://znanium.com/catalog/product/951294

5.3 Периодические издания:

Государство и право
Уголовное право
Российский следователь

6. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде организации и к профессиональным базам данных, электронным образовательным ресурсам, Интернет-сайтам специализированных ведомств.

Наименование сайта	Адрес сайта
Электронная библиотека диссертаций РГБ	http://diss.rsl.ru/
Национальная электронная библиотека	http://нэб.рф/
Электронный архив документов КубГУ	http://docspace.kubsu.ru
Федеральная служба государственной статистики	http://www.gks.ru
Территориальный орган Федеральной службы государственной статистики по Краснодарскому краю	http://www.krsdstat.ru
Президент Российской Федерации	http://kremlin.ru/
Совет Безопасности Российской Федерации	http://scrf.gov.ru/
Правительство Российской Федерации	http://government.ru/
Государственная Дума Федерального Собрания Российской Федерации	http://duma.gov.ru/
Совет Федерации Федерального Собрания Российской Федерации	http://council.gov.ru/
Сервер органов государственной власти Российской Федерации	http://gov.ru/
Служба внешней разведки Российской Федерации	http://svr.gov.ru/
Федеральная служба безопасности Российской Федерации	http://fsb.ru/
Генеральная прокуратура Российской Федерации	http://genproc.gov.ru/
Управление делами Президента Российской Федерации	http://udprf.ru/
Уполномоченный по правам человека в Российской Федерации	http://ombudsmanrf.ru/
Министерство иностранных дел Российской Федерации	http://mid.ru/
Конституционный Суд Российской Федерации	http://ksrf.ru/
Официальный интернет-портал правовой информации	http://pravo.gov.ru
Конституция Российской Федерации	http://constitution.ru/

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении дисциплины используются следующие формы работы.

1. Лекции, на которых рассматриваются основные теоретические вопросы данной дисциплины.

2. Практические занятия, на которых разбираются проблемные ситуации, решаются задачи, заслушиваются доклады, проводятся научные дискуссии, опрос по теоретическим вопросам изучаемых тем и тестирование. При подготовке к практическому занятию следует:

- использовать рекомендованные преподавателями учебники и учебные пособия - для закрепления теоретического материала;
- подготовить доклады и сообщения, разобрать проблемные ситуации;
- разобрать совместно с другими студентами и обсудить вопросы по теме практического занятия и т.д.

3. Самостоятельная работа, которая является одним из главных методов изучения дисциплины.

Цель самостоятельной работы – расширение кругозора и углубление знаний в области теории и практики вопросов изучаемой дисциплины.

Контроль за выполнением самостоятельной работы проводится при изучении каждой темы дисциплины на семинарских занятиях. Это текущий опрос, тестовые задания, подготовка рефератов.

Самостоятельная работа студента в процессе освоения дисциплины включает в себя:

– изучение основной и дополнительной литературы по курсу;
– работу с электронными библиотечными системами;
– изучение материалов периодической печати, Интернет - ресурсов;
– выполнение рефератов;
– индивидуальные и групповые консультации;
– подготовку к зачету.

3. Зачет по дисциплине. Зачет сдается в устной форме. Представляет собой структурированное задание по всем разделам дисциплины. Для подготовки к зачету следует воспользоваться рекомендованным преподавателем учебниками, методическими указаниями к практическим занятиям и самостоятельной контролируемой работе студента по дисциплине, глоссарием, своими конспектами лекций и практических занятий, выполненными самостоятельными работами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

8.1 Перечень информационных технологий

1. Проверка домашних заданий и индивидуальное консультирование посредством электронной почты.

8.2 Перечень необходимого программного обеспечения

При изучении дисциплины может быть использовано следующее программное обеспечение:

– комплекс взаимосвязанных программ, предназначенных для управления ресурсами ПК и организации взаимодействия с пользователем (операционная система Windows XP PRO);

– пакет приложений для выполнения основных задач компьютерной обработки различных типов документов (Microsoft Office 2003 PRO) в состав которого входят:

MS Word – текстовый процессор – для создания и редактирования текстовых документов;

MS Excel – табличный процессор – для обработки табличный данных и выполнения сложных вычислений;

MS Access – система управления базами данных – для организации работы с большими объемами данных;

MS Power Point – система подготовки электронных презентаций – для подготовки и проведения презентаций;

MS Outlook – менеджер персональной информации – для обеспечения унифицированного доступа к корпоративной информации;

MS FrontPage – система редактирования Web-узлов – для создания и обновления Web-узлов;

MS Publisher – настольная издательская система – для создания профессионально оформленных публикаций:

– программа для комплексной защиты ПК, объединяющая в себе антивирус, антишпион и функцию удаленного администратора (ESET Endpoint);

– пакет программ для создания и просмотра электронных публикаций в формате PDF (Adobe Reader);

– прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач (Google Chrome);

– программы, предназначенные для архивации, упаковки файлов путем сжатия хранимой в них информации (7zip).

8.3 Перечень информационных справочных систем

Обучающимся обеспечен доступ к современным профессиональным базам данных, справочным и поисковым системам.

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru).
2. Информационно-правовая система «Гарант» (http://www.garant.ru/)
3. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1	Занятия лекционного типа	Учебная аудитория с подключенным оборудованием (мультимедийный проектор, персональный компьютер, выход в Интернет, учебная мебель, доска учебная, учебно-наглядные пособия, обеспечивающие тематические иллюстрации)
2	Занятия семинарского типа	
3	Групповые и индивидуальные консультации	
4	Текущий контроль и промежуточная аттестация	
5	Самостоятельная работа	Кабинет оснащен компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета