МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Г.Ю. Нагорная
«31» 03 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности в правоохранительных органах

Уровень образовательной программы специалитет

Специальность 40.05.02 Правоохранительная деятельность

Специализация Оперативно-розыскная деятельность

Форма обучения очная (заочная)

Срок освоения ОП 5 лет (5 лет 9 месяцев)

Институт Юридический

Кафедра разработчик РПД Уголовно-правовые дисциплины

Выпускающие кафедры Государственно-правовые дисциплины, Гражданско-правовые дисциплины, Уголовно-правовые дисциплины

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института _____ Богатырева М.Р.

Заведующий кафедрой
«Государственно-правовые дисциплины» _____ Бекирова Ф.С.

И.о. зав. кафедрой
«Гражданско-правовые дисциплины» _____ Богатырева М.Р.

Заведующий кафедрой
«Уголовно-правовые дисциплины» _____ Чочуева З.А.

г. Черкесск, 2021 г.

СОДЕРЖАНИЕ

1. Цели освоения дисциплины……. 4
2. Место дисциплины в структуре образовательной программы.....4
3. Планируемые результаты обучения по дисциплине ……. 5
4. Структура и содержание дисциплины.....8
Объем дисциплины и виды учебной работы….....9
4.2. Содержание дисциплины ……... 9
4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля……. 9
4.2.2. Лекционный курс ……... 9
4.2.3. Лабораторный практикум ……..... 9
4.2.4. Практические занятия.....10
4.3. Самостоятельная работа обучающегося….....12
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....13
6. Образовательные технологии.....31
7. Учебно-методическое и информационное обеспечение дисциплины……. 32
7.1. Перечень основной и дополнительной учебной литературы……. 32
7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»…….. 33
7.3. Информационные технологии, лицензионное программное обеспечение 33
8. Материально-техническое обеспечение дисциплины …… 34
8.1. Требования к аудиториям (помещениям, местам) для проведения занятий 34
8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся 34
8.3. Требования к специализированному оборудованию…….. 34
9. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья…….. 26
Приложение 1. Фонд оценочных средств…….. 27
Приложение 2. Аннотация рабочей программы…….
Рецензия на рабочую программу……
Лист переутверждения рабочей программы дисциплины……

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины «Основы информационной безопасности в правоохранительных органах» является подготовка высококвалифицированных специалистов для работы в правоохранительных органах и иных организациях, способных представлять интересы в области международного информационного обмена, а также способных ориентироваться в проблемах формирования рынка информационных ресурсов и обеспечивать информационную безопасность государства, общества и личности; формирование у обучающихся представления об информационных отношениях; субъектах информационно-правовых отношений; о правовом режиме получения, передачи, хранения и использования информации; о юридических аспектах информационного обмена, информационной безопасности, ответственности в информационной сфере.

При этом задачами дисциплины являются:

- формирование у обучаемых понимание современных представлений о целях, задачах и практической программно-аппаратной реализации процесса обеспечения информационной безопасности профессиональной деятельности;
- обучить знаниям и умениям, позволяющим будущим специалистам безопасно ориентироваться и саморазвиваться в современном информационном пространстве, уметь защищать свои и служебные интересы в информационной сфере;
- привить будущим специалистам умения и навыки обеспечения информационной безопасности, необходимые для безопасного выполнения профессионально-служебных задач в едином информационном пространстве правоохранительных органов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности в правоохранительных органах» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули), имеет тесную связь с другими дисциплинами.

В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1.	Информатика и информационные технологии профессиональной деятельности	Судебная бухгалтерия Правовая статистика Тактико-специальная подготовка Информационное право

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями образовательного стандарта по специальности 40.05.02 Правоохранительная деятельность и формируются в соответствии с матрицей компетенций ОП

№ п/п	**Номер/ индекс компетенции**	**Наименование компетенции (или ее части)**	**В результате изучения дисциплины обучающиеся должны:**
1	**2**	**3**	**4**
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1.Анализирует задачу, выделяя ее базовые составляющие УК-1.2.Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи; УК-1.3.Осуществляет поиск информации для решения поставленной задачи по различным типам запросов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы		**Всего часов**	Семестры
			№4 часов
1		2	3
Аудиторная контактная работа (всего)		***54***	***54***
В том числе:			
Лекции (Л)		*18*	*18*
Практические занятия (ПЗ), Семинары (С)		*36*	*36*
Внеаудиторная контактная работа В том числе: индивидуальные и групповые консультации		*1,7*	*1,7*
Самостоятельная работа обучающегося (СРО) (всего)		***52***	***52***
Реферат (Реф)		*10*	*10*
Подготовка к занятиям (ПЗ)		*10*	*10*
Подготовка к промежуточному контролю (ППК)		*10*	*10*
Самоподготовка		*10*	*10*
Работа с книжными источниками		*12*	*12*
Промежуточная аттестация в том числе *СРО*	зачет (З)	*3*	*3*
	Прием зач., час	*0,3*	*0,3*
	СРО		
ИТОГО: Общая трудоемкость	**часов**	***108***	***108***
	зач. ед.	***3***	***3***

Заочная форма обучения

Вид учебной работы		Всего часов	Семестры
			№6 часов
1		2	3
Аудиторная контактная работа (всего)		***10***	***10***
В том числе:		-	-
Лекции		*4*	*4*
Практические занятия (ПЗ), Семинары (С)		*6*	*6*
Внеаудиторная контактная работа В том числе: индивидуальные и групповые консультации		*1*	*1*
Самостоятельная работа обучающегося (СРО) (всего)		***93***	***93***
Реферат (Реф)		*18*	*18*
Подготовка к занятиям (ПЗ)		*21*	*21*
Подготовка к промежуточному контролю (ППК)		*18*	*18*
Самоподготовка		*18*	*18*
Работа с книжными источниками		*18*	*18*
Промежуточная аттестация	зачет (З)	*3*	*3*
	Прием зач., час	*0,3*	*0,3*
	СРО	*3,7*	*3,7*
ИТОГО: Общая трудоемкость	**часов**	***108***	***108***
	зач. ед.	***3***	***3***

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Разделы дисциплины, виды деятельности и формы контроля

№ п/п	№ семестра	Наименование раздела дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации
			Л	**ЛР**	**ПЗ**	**СРО**	**всего**	
1	2	3	4	5	6	7	8	9
1.	4	Раздел 1. Уголовная ответственность за преступления в сфере компьютерной информации	2	-	6	10	18	*тестовый контроль, контрольные вопросы, реферат*

2.	4	Раздел 2. Информационный поиск при исследовании компьютера и доказательства по компьютерной информации	4	-	8	10	22	*тестовый контроль, контрольные вопросы, реферат*
3.	4	Раздел3. Биометрические средства ограничения доступа	4	-	6	10	20	*тестовый контроль, контрольные вопросы, реферат*
4.	4	Раздел 4. Защита информационных процессов в компьютерных системах	4	-	8	10	22	*тестовый контроль, контрольные вопросы, реферат*
5.	4	Раздел 5. Защита информации в телекоммуникационных системах	4	-	8	12	24	*тестовый контроль, контрольные вопросы, реферат*
6.	4	Внеаудиторная контактная работа					1,7	*В том числе: индивидуальные и групповые консультации*
7.	4	Промежуточная аттестация					0,3	*Зачет*
		ИТОГО:	18		36	52	108	

Заочная форма обучения

№ п/п	**№ семестра**	**Наименование раздела дисциплины**	**Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)**				**Формы текущей и промежуточной аттестации**
			Л	**ПЗ**	**СРО**	**всего**	
1	2	3	4	5	6	7	8
8.	4	Раздел 1. Уголовная ответственность за преступления в сфере компьютерной информации	2	4	18	24	*тестовый контроль, контрольные вопросы, реферат*

9.	4	Раздел 2. Информационный поиск при исследовании компьютера и доказательства по компьютерной информации			21	22	*тестовый контроль, контрольные вопросы, реферат*
10.	4	Раздел3. Биометрические средства ограничения доступа	2	2	18	22	*тестовый контроль, контрольные вопросы, реферат*
11.	4	Раздел 4. Защита информационных процессов в компьютерных системах			18	18	*тестовый контроль, контрольные вопросы, реферат*
12.	4	Раздел 5. Защита информации в телекоммуникационных системах			18	18	*тестовый контроль, контрольные вопросы, реферат*
13.	4	Внеаудиторная контактная работа	1			3,7	*В том числе: индивидуальные и групповые консультации*
14.	4	Промежуточная аттестация				0,3	*Зачет*
		ИТОГО:	5	6	93	108	

Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
Семестр 4 (6)					
1.	**Раздел 1** Уголовная ответственность за преступления в сфере компьютерной информации	**Тема 1.** Проблемы обеспечения информационной безопасности в правоохранительных органах. Основные термины, понятие, способы и средства защиты.	1. Особенности обеспечения информационной безопасности а ПО 2. Актуальность защиты информации в автоматизированных системах 3. Информационные отношения. Субъекты информационных отношений и их безопасность. 4. Способы и средства обеспечения безопасности	2	4

			информации		
2.	**Раздел 2** Информационный поиск при исследовании компьютера и доказательства по компьютерной информации	**Тема 1.** Правовые аспекты защиты информации организационно-правовые основы защиты информации.	1. Формирования законодательства в области информатизации в РФ 2. Стандарты и рекомендации в области информационной безопасности 3. Системы сертификации средств защиты информации 4. Стандарты безопасности информационных технологий 5. Преступления в сфере компьютерной информации	4	
3.	**Раздел 3** Биометрические средства ограничения доступа	**Тема 1.** Качество биометрической системы ограничения доступа. Пластиковые карты.	1.Биологические параметры, используемые в системах ограничения доступа. 3.Пластиковые карты как средство разрешения доступа или получения полномочий. 3.Виды и особенности различных пластиковых карт	4	
4.	**Раздел 4** Защита информационных процессов в компьютерных системах	**Тема 1.** Защита информационных процессов в компьютерных системах. Защита информации от утечки на объектах информатизации ПО	1.Потенциальный угрозы и каналы утечки информации на ПЭВМ 2.Цели и задачи систем компьютерной безопасности 3. Принципы построения систем защиты компьютерной информации 4.Обеспечение защиты информации на ПЭВМ 5.Защита информации от утечки на объектах информатизации ПО	4	
5.	**Раздел 5.** Защита информации в телекоммуникационных системах	**Тема 1.** Защита информации в телекоммуникационных системах	1.Основные понятия и классификация компьютерных сетей 2.Защита информации в информационных вычислительных сетях 3.Особенности получения доступа и использования доступа и использования информационных ресурсов сети интернет в системе ПО России	4	
	ИТОГО часов в семестре:			18	4

Лабораторный практикум - учебным планом не предусмотрен

Практические занятия

№ п/п	Наименование раздела (темы) дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
1.	**Раздел 1.** Уголовная ответственность за преступления в сфере компьютерной информации	**Тема 1.** Проблемы обеспечения информационной безопасности в правоохранительных органах. Основные термины, понятие, способы и средства защиты.	Подготовка к осмотру компьютерных средств. Предварительная ориентировка перед обыском или осмотром компьютерной техники. Отключение компьютерной системы и документирование. Изъятие компьютерных средств и транспортировка компьютера к месту хранения или исследования. Исследование и экспертиза по компьютерной аппаратуре и информации. Исследование, анализ и восстановление компьютерных данных. Виды хранящейся компьютерной информации. Подготовка исследования. Средства исследования компьютерных данных. Полное резервирование данных на диске (изъятие без выемки). Исследование по восстановленной копии бит-резервирования. Исследование резервных копий. Методы скрытого исследования.	4	6
2.	**Раздел 2** Информационный поиск при исследовании компьютера и доказательства по компьютерной информации	**Тема 1.** Правовые аспекты защиты информации организационно-правовые основы защиты информации.	Целесообразность автоматического поиска документов по параметрам. Обычный и расширенный поиск документов, индексирование. Расширенный поиск документов по содержанию и свойствам файлов с формированием логических условий на текст, имя, тип файла и другие свойства. Панель поиска в области задач программ пакета MicrosoftOffice. Программа Поиск файлов, автоматическое создание индекса (база данных свойств и слов по документам на дисках). Специализированные настольные поисковые системы с индексированием и безиндексирования YandexDesktopSearch, Find-Бульдозер, Архиватор 3000, AVSearch, SuperiorSearch. Интерфейс, модули типов файлов. Исследование файлов и компьютерных документов. Поиск информации в файлахпо реквизитам, по содержанию текста, индексный поиск. Расширенный поиск по условиям. Поиск в графических файлах. Файлы результатов сканирования. Исследование файлов текстовых	2	

			документов и записок, табличных данных. Графология компьютерного текстового набора.		
		Тема 2. Форматы и реквизиты файлов	Технологические и служебные сведения в файлах. Виды русской кодировки. Информация по списку файлов документов последних сеансов работы. Исследование электронной почты. Особенности эксплуатации электронной почты, внутренняя и внешняя переписка. Журнал почты. Исследование почтовых папок сообщений и прикрепленных файлов. Исследование писем, получаемых через почтовые веб-сайты. Выяснение отправителя почтового письма. Информация из программ планировщиков и ежедневников. Поиск в базах данных. Исследование работы пользователя в Интернете. Журнал истории работы в Интернете, закладки. Исследование кэша работы в Интернете.	2	
		Тема 3. Исследование сетевого проникновения к компьютерной информации	Особенности эксплуатации компьютерной сети. Прокси-серверы. Выяснение обстоятельств проникновения в сетевую систему. Изучение сетевого администрирования, защиты, правил работы. Администратор сети. Файлы истории работы в сети (log-файлы), виды, обслуживание и исследование. Исследование работы сотрудников и пользователей в локальной сети и Интернете. Сведения о посетителе Интернета и Web-страниц. Следственные действия с лицом, подозреваемым во взломе сети. Правовая ответственность поставщика сетевых услуг и сведения, которые он может предоставить. Исследование преступлений в финансовой сфере с компьютерной информацией Современные информационные технологии и сети в финансовой и экономической сфере. Электронная документация, цифровая подпись. Кредитные карты. Электронная коммерция и торговля.	2	
		Тема 4. Доказывание и доказательства по компьютерной информации	Протоколы и показания по компьютерным преступлениям. Стандартные термины постановлений, протоколов и показаний. Постановление об осмотре данных или запрос (письмо) в организацию в связи с предстоящим осмотром. Особенности подготовки материалов по	2	

			компьютерным преступлениям для представления в суде. Современные методы судебной экспозиции материалов.		
3.	**Раздел 3**. Биометрические средства ограничения доступа	Тема 1. Качество биометрической системы ограничения доступа. Пластиковые карты.	Качество биометрической системы ограничения доступа. Биологические параметры, используемые в системах ограничения доступа. Идентификационные задачи, решаемые аппаратурой биометрического контроля Пластиковые карты как средство разрешения доступа или получения полномочий. Виды и особенности различных пластиковых карт.	2	
		Тема 2. Кодирование и перекодирование информации. Пароли.	Кодирование информации, вводимой в компьютер. Понятие кодовой таблицы (страницы) Тип (формат или расширение имени файла) как признак определенной кодировки. Перекодирование стандартными и офисными программами. Перекодирование и создание собственной кодировки специальными программами Понятие и назначение пароля; объекты, доступ к которым ограничивают пароли. Современные требования к составлению паролей. Классификация паролей. Виды атак на пароли. Способы запоминания надежных паролей.	2	
		Тема 3. Защита документов, подготовленных в текстовом редактор MsWord Защита документов, подготовленных в табличном процессоре MsExcel	Парольная защита файлов с документами. Криптографическая защита. Режимная защита. Стенографическая защита. Цифровая подпись документа. Способы преодоления защиты документа или файла. Объекты защиты в MS Excel. Особенности режимной защиты в MS Excel. Создание частично защищаемых объектов на примере защиты листа. Скрытие объектов в MS Excel. Способы преодоления защиты.	2	
		Тема 4. Защита html-документов и веб-сайтов	Особенности «строения» HTML-документа. Объекты, требующие защиты. Способы защиты отдельных частей HTML-документа. Потенциально опасные теги в документе. Особенности защиты компилированных документов (формата CHM или	2	

			электронной книги).		
4.	**Раздел 4** Защита информационных процессов в компьютерных системах.	Тема 1. Защита информационных процессов в компьютерных системах. Защита информации от утечки на объектах информатизации ПО. Защита носителей информации	От каких «воздействий» необходимо защищать программы? Юридические виды распространения программ. Механизмы защиты программ. Шифрование и упаковка программ. Полезные советы по защите программ. Защита структур (файлов и папок), сохраняемых на носителях. Контейнерная защита. Защита дискет. Защита CD-ROM, DVD. Региональная защита DVD.	2	
		Тема 2. Организация защиты в сети	Виды и структуры сетей. Основные принципы организации конкретных атак. Доверительность отношений в сетевом обмене. Аутентификация пользователей. Протоколы аутентификации. Виртуальные защищенные каналы связи.	2	
		Тема 3. Электронная подпись и защита электронных сделок	Способы преобразования информации при сетевом обмене (архивирование – сжатие, перекодирование, шифрование, кэширование). Допустимость электронных сделок. Нотариальное заверение документов. Электронное заверение документов. Различные способы использования электронной подписи	2	
		Тема 4. Защита персональных данных	Общедоступные персональные данные. Обезличивание персональных данных. Понятие и обязанности оператора. Особенности отношений субъекта персональных данных и оператора.	2	
5.	**Раздел 5** Защита информации в телекоммуникационных системах	Тема1. Защита информации в информационных вычислительных сетях	1.Основные понятия и классификация компьютерных сетей 2.Защита информации в информационных вычислительных сетях 3.Особенности получения доступа и использования доступа и использования информационных ресурсов сети интернет в системе ПО России	8	
	Всего часов в семестре:			36	6

САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов	
				ОФО	ЗФО
1	3	4	5	6	
Семестр 4 (6)					
1.	**Раздел 1** Уголовная ответственность за преступления в сфере компьютерной информации	1.1.	*Реферат (Реф)*	2	4
		1.2	*Подготовка к занятиям (ПЗ)*	2	5
		1.3	*Подготовка к промежуточному контролю (ППК)*	2	4
		1.4	*Самоподготовка*	2	4
		1.5	*Работа с книжными источниками*	2	4
2.	**Раздел 2** Информационный поиск при исследовании компьютера и доказательства по компьютерной информации	2.1.	*Реферат (Реф)*	2	4
		2.2.	*Подготовка к занятиям (ПЗ)*	2	5
		2.3.	*Подготовка к промежуточному контролю (ППК)*	2	4
		2.4	*Самоподготовка*	2	4
		2.5	*Работа с книжными источниками*	2	4
3.	Раздел 3. Биометрические средства ограничения доступа	3.1.	*Реферат (Реф)*	2	4
		3.2.	*Подготовка к занятиям (ПЗ)*	2	5
		3.3.	*Подготовка к промежуточному контролю (ППК)*	2	4
		3.4	*Самоподготовка*	2	4
		3.5	*Работа с книжными источниками*	2	4
4.	Раздел 4. Защита информационных процессов в компьютерных системах.	4.1	*Реферат (Реф)*	2	4
		4.2	*Подготовка к занятиям (ПЗ)*	2	4
		4.3	*Подготовка к промежуточному контролю (ППК)*	2	4
		4.4	*Самоподготовка*	2	4
		4.5	*Работа с книжными источниками*	2	2
	Раздел 5. Защита информации в телекоммуникационных системах	5.1	*Реферат (Реф)*	2	2
		5.2	*Подготовка к занятиям (ПЗ)*	2	2
		5.3	*Подготовка к промежуточному контролю (ППК)*	2	2
		5.4	*Самоподготовка*	2	2
		5.5	*Работа с книжными источниками*	2	4
Всего часов в семестре:				**50**	**93**

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Методические указания для подготовки обучающихся к лекционным занятиям

Обучающимся необходимо ознакомиться:

- с содержанием рабочей программы дисциплины (далее - РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине.

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой обучающихся всегда находится в центре внимания кафедры.

Обучающимся необходимо:

- перед каждой лекцией просматривать рабочую программу

дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;

- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;

- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях. Не оставляйте «белых пятен» в освоении материала.

Методические указания для подготовки обучающихся к практическим занятиям

Обучающимся следует:

- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

- при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно- правовые акты и материалы правоприменительной практики;

- теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;

- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

- в ходе практического занятия давать конкретные, четкие ответы по существу вопросов;

- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Обучающимся, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется явиться на консультацию к преподавателю и отчитаться по теме, изучавшийся на занятии. Обучающиеся, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме дисциплины обучающимся предлагается перечень заданий для самостоятельной работы.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

- руководствоваться графиком самостоятельной работы, определенным РПД;
- руководствоваться графиком самостоятельной работы, определенным РПД;
- при подготовке к зачету параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на плановой консультации.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	№ семестра	Виды учебной работы	Образовательные технологии	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
1.	4	Лекция: Проблемы обеспечения информационной безопасности в правоохранительных органах. Основные термины, понятие, способы и средства защиты.	*Использование технических средств (проектора, ноутбука) для материала в виде презентаций.*	*2*	*6*
2.	4	Лекция: Правовые аспекты защиты информации организационно-правовые основы защиты информации.	*Использование технических средств (проектора, ноутбука) для материала в виде презентаций.*	*4*	
3.	4	Лекция: Качество биометрической системы ограничения доступа. Пластиковые карты.	*Использование технических средств (проектора, ноутбука) для материала в виде презентаций.*	*4*	
4.	4	Лекция: Защита информационных процессов в компьютерных системах. Защита информации от утечки на объектах информатизации ПО	*Использование технических средств (проектора, ноутбука) для материала в виде презентаций.*	*4*	
5.	4	Лекция: Защита информации в телекоммуникационных системах	*Использование технических средств (проектора, ноутбука) для материала в виде презентаций.*	*4*	
6.	4	Практическое занятие: Защита информационных процессов в компьютерных системах. Защита информации от утечки на объектах информатизации ПО	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*4*	

7.	4	Практическое занятие: Защита информации в телекоммуникационных системах	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций е.*	*4*	
8.	4	Практическое занятие: Защита документов подготовленных в пакете прикладных программ Microsoft Officce	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*4*	
9.	4	Практическое занятие: Форматы и реквизиты файлов	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций.*	*4*	
10.	4	Практическое занятие: Защита html-документов и веб-сайтов	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*2*	
11.	4	Практическое занятие: Защита исполняемых программ и носителей информации	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*4*	
12.	4	Практическое занятие: Биометрические средства ограничения доступа	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*2*	
13.	4	Практическое занятие: Кодирование и перекодирование информации	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*4*	
14.	4	Практическое занятие: Пароли	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*4*	
15.	4	Практическое занятие: Электронная подпись и защита электронных сделок	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*2*	
16.	4	Практическое занятие :Защита персональных данных	*Работа в компьютерном классе. Подготовка реферата, подготовка к презентаций*	*2*	

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень основной и дополнительной учебной литературы

1. Молдованова, О. В. Информационные системы и базы данных : учебное пособие / О. В. Молдованова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2014. — 178 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/45470.html
2. Информационные технологии в юридической деятельности : учебное пособие для студентов вузов, обучающихся по специальностям «Юриспруденция» и «Правоохранительная деятельность» / С. Я. Казанцев, Н. М. Дубинина, А. И. Уринцов [и др.] ; под редакцией А. И. Уринцова. — 2-е изд. — Москва : ЮНИТИ-ДАНА, 2020. — 352 с. — ISBN 978-5-238-03242-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/109189.html
3. Шевко, Н. Р. Информационные технологии в юридической деятельности : учебное пособие / Н. Р. Шевко, С. Я. Казанцев, О. Э. Згадзай ; под редакцией С. Я. Казанцева. — Казань : Казанский юридический институт МВД России, 2016. — 230 с. — ISBN 978-5-901593-69-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/86477.html
4. Мистров, Л. Е. Информационные технологии в юридической деятельности. Microsoft Office 2010 : учебное пособие / Л. Е. Мистров, А. В. Мишин. — Москва : Российский государственный университет правосудия, 2016. — 232 с. — ISBN 978-5-93916-503-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/65857.htm

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Российская газета http://www.rg.ru/
2. Журналы: Административное право, Горячая линия бухгалтера, Делопроизводство, Жилищное право, Мастер продаж, Секретарское дело, Трудовое право http://www.top-personal.ru/
3. Газета «Учет, налоги, право» http://www.gazeta-unp.ru/
4. Журнал «Домашний адвокат» http://www.bestlawyers.ru/jr/jr.html
5. Российский юридический журнал http://www.ruzh.org/

7.1 Информационные технологии

Программное обеспечение используемое в учебных целях

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
1.Windows 7, 8, 8.1, 10 2. Access 2007, 2010, 2013	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022 (продление подписки)
S Office 2003, 2007, 2010, 2013	Сведения об OpenOffice: 63143487, 63321452, 64026734, 6416302, 64344172, 64394739, 64468661, 64489816, 64537893, 64563149, 64990070, 65615073 Лицензия бессрочная
Антивирус Dr.Web Desktop Security Suite	Лицензионный сертификат Серийный № 8DVG-V96F-H8S7-NRBC Срок действия: с 20.10.2022 до 22.10.2023
Консультант Плюс	Договор № 272-186/С-23-01 от 20.12.2022 г.
Цифровой образовательный ресурс IPRsmart	Лицензионный договор № 9368/22П от 01.07.2022 г. Срок действия: с 01.07.2022 до 01.07.2023
SumatraPDF, 7-Zip.	Бесплатное ПО

8. МАТЕРИАЛЬНО - ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Требования к аудиториям (помещениям, местам) для проведения занятий:

Учебная аудитория для проведения занятий лекционного типа

Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации:

Специализированная мебель:

Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Мультимедийный проектор -1 шт.
Экран -1 шт.
Специализированная мебель:
Столы ученические – 11 шт.
Стулья ученические – 22 шт.
Стул полумягкий– 1 шт.
Тумба кафедра – 1 шт.
Доска ученическая – 1 шт.
Стол двухтумбовый -1 шт.
Шкаф двухдверный – 1 шт.
Жалюзи вертикальные – 2 шт.
Зеркало – 1 шт.
Бактерицидный рециркулятор -1 шт.

Учебная аудитория для проведения занятий практического типа, курсового проектирования (выполнение курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Специализированная мебель:
Доска ученическая, шкаф книжный, компьютерные столы, шкаф для одежды, стулья; стол; кафедра.

Помещение для самостоятельной работы:

Библиотечно-издательский центр
Отдел обслуживания электронными изданиями

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду ФГБОУ ВО «СевКавГА»:

1. Персональный компьютер;
2. Сканер;
3. МФУ.

Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок.

Помещение для самостоятельной работы

1. **Библиотечно-издательский центр (БИЦ)**

Комплект проекционный, мультимедийный интерактивный IQ Board DVT:
интерактивная доска 84” IQ Board DVT T084,
проектор TRIUMPH PJ1000
универсальное настенное крепление
Wize WTH140
Персональный компьютер-моноблок MSI AE202072 - 18 шт.
Персональный компьютер Samsung – 1 шт.
Специализированная мебель):
Столы на 1 рабочее место – 20 шт
Столы на 2 рабочих места – 9 шт
Стулья – 38 шт
МФУ Sharp AR-6020 – 1 шт.
Brother DCR-1510R – 1 шт.
Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок

2. **Электронный читальный зал**

Комплект проекционный, мультимедийный интерактивный IQ Board DVT:
интерактивная доска 84” IQ Board DVT T084,
проектор TRIUMPH PJ1000
универсальное настенное крепление
Wize WTH140
Персональный компьютер-моноблок MSI AE202072 - 18 шт.
Персональный компьютер Samsung – 1 шт.
Специализированная мебель):
Столы на 1 рабочее место – 20 шт
Столы на 2 рабочих места – 9 шт
Стулья – 38 шт
МФУ Sharp AR-6020 – 1 шт.
Brother DCR-1510R – 1 шт.
Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок

3. **Читальный зал**

Специализированная мебель:
Столы на 2 рабочих места – 12 шт.
Стулья – 24 шт.
Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок

4. **Библиотечно-издательский центр (БИЦ)**

Отдел обслуживания печатными изданиями
Ауд. № 1

Комплект проекционный, мультимедийный оборудование:
Экран настенный Screen Media 244/244 корпус 1106
Проектор BenG MX660P 1024/7683200 LM
Ноутбук Lenovo G500 15.6''
Рабочие столы на 1 место – 21 шт.
Стулья – 55 шт.
Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок

5. **Отдел обслуживания электронными изданиями**
Ауд. № 9

Специализированная мебель (столы и стулья):
Рабочие столы на 1 место – 24 шт.
Стулья – 24 шт.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ФГБОУ ВО «СевКавГА»:
Монитор Acer TFT 19 – 20 шт.
Монитор ViewSonic - 1 шт.
Сетевой терминал Office Station -18 шт.
Персональный компьютер Samsung -3 шт.
МФУ Canon 3228(7310) – 1 шт.
МФУ Sharp AR-6020 – 1 шт.
Принтер Canon i -Sensys LBP 6750 dh – 1 шт.
Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок

6. **Информационно-библиографический отдел**
Ауд. № 8

Специализированная мебель:
Рабочие столы на 1 место- 6 шт.
Стулья- 6 шт.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ФГБОУ ВО «СевКавГА»:
Персональный компьютер – 1шт.
Сканер Epson Perfection 2480 photo
МФУ MFC 7320R
Выделенные стоянки автотранспортных средств для инвалидов; поручни; пандусы; достаточная ширина дверных проемов в стенах, лестничных маршей, площадок

Требования к оборудованию рабочих мест преподавателя и обучающихся:
1. Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.
2. Рабочие места обучающихся, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Требования к специализированному оборудованию

- нет

9. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается (в случае необходимости) адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения материала для лекционных и практических занятий.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья комплектуется фонд основной учебной литературы и электронных образовательных ресурсов, адаптированных к ограничению их здоровья, доступ к которым организован в БИЦ ФГБОУ ВО «СевКавГА». В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ: Основы информационной безопасности в правоохранительных органах

1.ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Основы информационной безопасности в правоохранительных органах»

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода,вырабатывать стратегию действий

2. Этапы формирования компетенции в процессе освоения дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающимися.

Этапность формирования компетенций прямо связана с местом дисциплины в образовательной программе.

Разделы (темы) дисциплины	**Формируемые компетенции (коды)**
	УК-1
Проблемы обеспечения информационной безопасности в правоохранительных органах. Основные термины, понятие, способы исредства защиты.	+
Правовые аспекты защиты информации организационно-правовыеосновы защиты информации.	+
Защита информации криптографическими методами	+
Защита информационных процессов в компьютерных системах. Защита информации от утечки на объектах информатизации ПО	+
Защита информации в телекоммуникационных системах	+
Защита документов подготовленных в пакете прикладных программ MicrosoftOfficce	+
Форматы и реквизиты файлов	+
Защита html-документов и веб-сайтов	+
Защита исполняемых программ и носителей информации	+
Биометрические средства ограничения доступа	+
Кодирование и перекодирование Информации	+
Пароли	+

Электронная подпись и защита электронных сделок	+
Защита персональных данных	+

3. Показатели, критерии и средства оценивания компетенций, формируемых в процессе изучения дисциплины

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Индикаторы достижения компетенции	**Неудовлетв.**	**Удовлетв.**	**хорошо**	**отлично**	**Текущий контроль**	**Промежуточная аттестация**
УК-1**.**1 Анализирует задачу, выделяя ее базовые составляющие	Не умеет анализировать задачу, выделяя ее базовые составляющие	Частично умеет анализировать задачу, выделяя ее базовые составляющие	Хорошо умеет анализировать задачу, выделяя ее базовые составляющие	Отлично анализирует задачу, выделяя ее базовые составляющие	*тестовый контроль, контрольные вопросы, реферат*	зачет
УК-1.2.Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи;	Не умеет Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи;	. Частично умеет Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи;	Хорошо умеет Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи;	Отлично Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи;	*тестовый контроль, контрольные вопросы, реферат*	зачет
УК-1.3**.**Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	*тестовый контроль, контрольные вопросы, реферат*	зачет

Вопросы к зачету
по дисциплине «Основы информационной безопасности в правоохранительных органах»

1. Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.
2. Основные составляющие национальных интересов в информационной сфере.
3. Виды и источники угроз информационной безопасности страны (на примере России).
4. Принципы государственной политики обеспечения информационной безопасности страны (на примере Российской Федерации).
5. Информационная сфера и информационная безопасность правоохранительных органов.
6. Обеспечение информационной безопасности в процессе деятельности оперативных подразделений органов внутренних дел.
7. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности правоохранительных органов.
8. Защита информации. Комплексный подход к защите информации.
9. Классификация методов защиты информации.
10. Понятие и виды каналов утечки информации ограниченного доступа. «Типовые» каналы утечки информации объектов информатизации ПО.
11. «Типовые» каналы утечки информации объектов информатизации ПО. Условия и факторы, способствующие утечке информации ограниченного доступа.
12. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.
13. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки.
14. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты.
15. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки.
16. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.
17. Уязвимость компьютерных систем. Понятие несанкционированного доступа. Классы и виды несанкционированного доступа.
18. Уязвимость компьютерных систем. Модель злоумышленника.
19. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов.
20. Методы и средства защиты данных от несанкционированного доступа.
21. Основные методы НСД при физическом контакте с компьютером.
22. Классический алгоритм поведения злоумышленника при удаленном несанкционированном доступе в компьютерную систему.
23. Основные причины утечки информации с охраняемых объектов.
24. Разграничение доступа к информации. Идентификация и аутентификация.
25. Криптографические методы защиты данных. Электронно-цифровая подпись.
26. Основные угрозы безопасности информации в компьютерных системах.
27. Вредоносные программы и методы борьбы с ними.
28. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.
29. Методы и средства воздействия на безопасность сетей.

30. Особенности построения защиты информации в телекоммуникационных сетях. Современные технические и программные средства сетевой защиты компьютерной информации.
31. Применение электронно-цифровой подписи для защиты документов.
32. Идентификация электронных и бумажных документов. Реквизиты и свойства документов.
33. Свойства файла и свойства электронного документа.
34. Свойства электронного документа – фиксация в электронном документе и в бумажной форме.
35. Свойства электронного документа – поиск документов по заданному фрагменту текста.
36. Свойства электронного документа – поиск документов по заданным свойствам.
37. Понятие и назначение шаблона процессуальных документов.
38. Создание нового шаблона на основе одного из стандартных шаблонов MS Word.
39. Создание нового шаблона на основе готового электронного документа.
40. Извлечение и использование готовых шаблонов процессуальных документов изстандартных шаблонов MS Word.
41. Сохранение шаблонов и создание на их основе новых документов.
42. Автоматизация заполнения электронных документов. Создание защищенного шаблона
43. Виды и параметры полей форм. Текстовое поле, флажок, список.
44. Понятие и места установки паролей.
45. Современные требования к надежным паролям.
46. Виды атак на пароли и классификация паролей.
47. Правила составления и запоминания надежных (сложных) паролей.
48. Парольная защита документов MS Word. Установка и различные виды парольной защиты.
49. Возможности преодоления и обхода парольной защиты документов MS Word.
50. Приемы скрытия текста и графических объектов в документе.
51. Приемы обнаружения скрытых текстовых и графических объектов в документе.
52. Защита различных объектов в MS Excel: книги, листа, ячейки, выделенного диапазона.
53. Создание защищенной таблицы с редактируемыми областями.
54. Скрытие объектов в Excel: окна Excel, окна книги, листов, ячеек, выделенных диапазонов, формул.
55. Приемы скрытия текста и графических объектов в документе MS Excel.
56. Приемы обнаружения скрытых текстовых и графических объектов в документе MS Excel.
57. Шифрование любых файлов с документами.
58. Добавление текстовой информации в конец графического файла.
59. Запаковка текста внутри графического файла с искажением последнего.
60. Сокрытие текста внутри графического файла без искажения последнего.
61. Понятие и квалификация преступлений в сфере компьютерной информаций

Темы рефератов
по дисциплине «Основы информационной безопасности в правоохранительных органах»

1. Классификация вредоносных программ и защита от их воздействия.
2. Темы и шаблоны в Microsoft Office Word как средства профессионального оформления документов.
3. Применение полей Microsoft Office Word в электронном делопроизводстве.
4. Поля Microsoft Office Word как средство быстрого извлечения информации.
5. Возможности Microsof tOffice Word по защите и разграничению доступа при работе в корпоративной сети.
6. Создание формв Microsoft Office Word, Excel, Access.
7. Средства электронной подготовки и обработки документов бланкового типа.
8. Обеспечение безопасности и защита документов Microsoft Office Word.
9. Форматы файлов и преобразование документов в Microsoft Office Word.
10. Система защиты информации в России
11. Правовые способы защиты информации в России
12. Угроза информационной безопасности от вредоносных программ
13. Защита информации от вредоносных программ
14. Угрозы неприкосновенности личного пространства человека с развитие информационных технологий и Интернета.
15. Информационное неравенство, цифровое разделение общества, информационная бедность. Проблемы, последствия, пути решения.
16. Политика безопасности и информационной безопасности России
17. Информационные риски (опасность возникновения убытков или ущерба в результате применения информационных технологий, ИТ-риски).
18. Информационная война и агрессивная политика в Интернете (определение, в отношении своей страны, другой страны, цели, формы, примеры, терроризм, национализм, религиозный фанатизм).
19. Последствия развития Интернета в современных государствах. Основные угрозы со стороны Интернета для современного государства (в частности, политические и экономические).
20. Подходы к государственному регулированию Интернета в России и других государствах. Мероприятия и законодательные инициативы.
21. Растущие угрозы компьютерной безопасности как следствие коммерциализации Интернета.

Комплект тестовых вопросов

по дисциплине «Основы информационной безопасности в правоохранительных органах»
Компетенции, формируемые в процессе изучения дисциплины
(УК-1)

1. «Разъяснение, представление, понятие о чём-либо» сведения (сообщения, данные) независимо от формы их представления -это…….

2. Интерпретация информации – это
   - переход к семантическому смыслу.
   - переход к синтаксическому смыслу.
   - расшифровка информации
   - искажение информации

3. Какого типа бывает информации по отношению к источнику или приемнику
   - входная, выходная и внутренняя
   - исходная, промежуточная и результирующая
   - постоянная, переменная и смешанная
   - первичная и вторичная

4. 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 –это……..

5. Информация по ее изменчивости бывает:
   - входная, выходная и внутренняя
   - исходная, промежуточная и результирующая
   - постоянная, переменная и смешанная
   - первичная и вторичная

6. Информация по ее полноте бывает:
   - избыточная, достаточная и недостаточная
   - открытая (общедоступная) и закрытая (конфиденциальная)
   - входная, выходная и внутренняя
   - исходная, промежуточная и результирующая

7. Информация по доступу к ней бывает:
   - открытая (общедоступная) и закрытая (конфиденциальная)
   - избыточная, достаточная и недостаточная
   - исходная, промежуточная и результирующая
   - постоянная, переменная и смешанная

8. Комплекс мероприятий, направленных на обеспечение информационной безопасности это……..

9. Информация, которая не зависит от личного мнения или суждения, называется:
   - достоверной
   - актуальной
   - объективной
   - полезной
   - понятной

10. Информационное право составляет:
    - нормативную базу информационного общества

- государственную политику
- нормативную базу аграрного общества
- нормативную базу до индустриального общества

11. Регистрация доменных имён, содержащих торговую марку, принадлежащую другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования -это ……..

12.Обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей –это……..

- контрольный чек
- ярлык
- обозначение, служащее для индивидуализации товаров
- договор купли-продажи

13.Информационные ресурсы по виду информации:

- политическая
- конфиденциальная
- передвижная
- на бумажном носителе

14.Основными техническими средствами являются:

- средства связи и телекоммуникаций
- прикладный программы
- операционные системы
- словари

15.Программа просмотра гипертекстовых страниц WWW:

- браузер
- протокол
- сервер
- HTML

16.Вспомогательное приспособление, позволяющее точнее провести какое-либо действие – это…….

17.Передача имущественных прав может осуществляться

- на основе судебного иска
- на основе авторского договора
- без авторского договора

18. Кто является основным ответственным за определение уровня классификации информации

- Руководитель среднего звена
- Высшее руководство
- Владелец
- Пользователь

19. Укажите субъектов доступа к информации:

- Носитель
- Потребитель
- Накопитель
- Собственник
- Владелец

20.Выбери правильный ответ

- На чем основан принцип работы антивирусных мониторов:
- На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю
- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
- На подсчете контрольных сумм для присутствующих на диске файлов или

системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

21.Выбери правильный ответ

На чем основан принцип работы антивирусных иммунизаторов:

- На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные
- На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
- На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.
- На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю

22.Выбери правильный ответ

Что необходимо сделать при обнаружении файлового вируса?

- Компьютер необходимо отключить от сети и проинформировать системного администратора
- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

23.Выбери правильный ответ

Что необходимо сделать при обнаружении загрузочного вируса:

- Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
- Компьютер необходимо отключить от сети и проинформировать системного администратора
- Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

24.Выбери правильный ответ

В чем заключается метод защиты - ограничение доступа:

- В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
- В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
- В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
- В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. приведении её к неявному виду.

25. Несанкционированное копирование информации -это……..

26. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название

- Токен
- Password
- Login

- Смарт-карта
- Пароль

27. Компьютерная справочная правовая система в России- это……

28. Набор программ, которые управляют структурой БД и контролируют доступ к данным, хранящимся в БД-это……

29. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- Владельцы данных
- Пользователи
- Администраторы
- Руководство

30. К посторонним лицам нарушителям информационной безопасности относится: представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

- персонал, обслуживающий технические средства;
- технический персонал, обслуживающий здание;
- пользователи;
- сотрудники службы безопасности.
- представители конкурирующих организаций.
- лица, нарушившие пропускной режим. **(УК-1)**

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ КОМПЕТЕНЦИИ

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра.

К достоинствам данного типа относится его систематичность, непосредственно коррелирующаяся с требованием постоянного и непрерывного мониторинга качества обучения, а также возможность оценки успеваемости обучающихся.

Основными формами текущего контроля по дисциплине являются устный опрос, тестовый контроль, рефераты.

Форма итоговой аттестации – зачет.

Текущий контроль и промежуточная аттестация традиционно служат основным средством обеспечения в учебном процессе «обратной связи» между преподавателем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики преподавания дисциплин.

КРИТЕРИИ ОЦЕНКИ ЗАЧЕТОВ:

- **оценка «зачтено»** выставляется обучающимся, показавшим знание основного учебного материала в объеме, необходимом для дальнейшей учебы и в предстоящей работе по профессии, справляющихся с выполнением заданий, предусмотренных программой, но допустившим погрешности в ответе на экзамене и при выполнении контрольных заданий, не носящие принципиального характера, когда установлено, что обучающийся обладает необходимыми знаниями для последующего устранения указанных погрешностей под руководством преподавателя;
- **оценка «не зачтено»** выставляется обучающимся, обнаружившим пробелы в знания основного учебного материала, допускающим принципиальные ошибки в выполнении предусмотренных программой заданий. Такой оценки заслуживают ответы обучающихся, носящие несистематизированный, отрывочный, поверхностный характер, когда обучающийся не понимает существа излагаемых им вопросов, что свидетельствует о том, что обучающийся не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

КРИТЕРИИ ОЦЕНКИ РЕФЕРАТОВ:

- Оценка «отлично» выставляется, если выполнены все требования к написанию и защите реферата: обозначена рассматриваемая проблема и изложен современный взгляд на проблему (новые методы диагностики и лечения), сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

- Оценка «хорошо» выставляется, если основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; не в полной мере изложен современный взгляд на проблему (новые методы диагностики и лечения); не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны не полные ответы.

- Оценка «удовлетворительно» выставляется, если имеются существенные отступления от требования к реферированию. В частности: тема освещена лишь частично;

допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

- Оценка «неудовлетворительно» выставляется, если тема рефератов не раскрыта, обнаруживается существенное непонимание проблемы.

Критерии оценки тестовых заданий:

- От 0 до 59,9% выполненного решения –неудовлетворительно;
- От 60% до 79,9 –удовлетворительно;
- От 80% до 89,9%-хорошо
- От 90%до 100-отлично