Министерство культуры Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КРАСНОДАРСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ»
Информационно-библиотечный факультет
Кафедра библиотечно-библиографической деятельности и информационных технологий

УТВЕРЖДАЮ
зав. кафедрой библиотечно-библиографической деятельности и информационных технологий
_____Л.С. Финогина
«26» августа 2020 г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.ДВ.03.02 Защита информации и информационная безопасность в библиотеке

Направление подготовки 51.03.06 «Библиотечно-информационная деятельность»

Профиль подготовки «Менеджмент библиотечно-информационной деятельности»

Квалификация (степень) выпускника – бакалавр

Форма обучения – очная, заочная

Год начала подготовки – 2020

Краснодар
2020

Рабочая программа учебной дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность», утвержденным приказом Министерством образования и науки РФ от 6 декабря 2017 года № 1182 и основной профессиональной образовательной программой.

Рецензенты:

Заслуженный работник культуры РФ, Директор Централизованной библиотечной системы г. Краснодара — Е.А. Мирошниченко

Доктор пед. наук, профессор ФГБОУ ВО «Краснодарский государственный институт культуры» — Н.Б. Зиновьева

Составитель: Грушевская Н.В., ст. преподаватель кафедры ББДиИТ , канд. пед. наук

Рабочая программа учебной дисциплины «Защита информации и информационная безопасность в библиотеке» рассмотрена и утверждена на заседании кафедры ББДиИТ от «26» августа 2020 г. протокол № 1.

Рабочая программа учебной дисциплины «Защита информации и информационная безопасность в библиотеке» одобрена и рекомендована к использованию в учебном процессе Учебно-методическим советом ФГБОУ ВО «КГИК» «26» августа 2020 г. протокол № 1.

Содержание

1. Цели и задачи освоения дисциплины 4

2. Место дисциплины в структуре ОПОП ВО 4

3. Планируемые результаты обучения по дисциплине, соотнесенные с установленными в образовательной программе индикаторами достижения компетенций 4

4. Структура и содержание и дисциплины 5

4.1. Структура дисциплины: 5

4.2. Тематический план освоения дисциплины по видам учебной деятельности и виды самостоятельной (внеаудиторной) работы 6

5. Образовательные технологии 21

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации: 22

6.1. Контроль освоения дисциплины

6.2. Оценочные средства

7. Учебно-методическое и информационно обеспечение дисциплины (модуля) 29

7.1. Основная литература 23

7.2. Дополнительная литература 23

7.3. Периодические издания. 25

7.4. Интернет-ресурсы. 25

7.5. Методические указания и материалы по видам занятий 25

7.6. Программное обеспечение. 26

8. Материально-техническое обеспечение дисциплины (модуля) 26

9. Дополнения и изменения к рабочей программе учебной дисциплины (модуля) 27

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины (модуля)

- освоение методики и технологий защиты информации и информационной безопасности;

Задачи:

- изучить виды доступа к информации
- рассмотреть способы защиты информации
- выяснить методы шифрования и дешифрования информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к элективным дисциплинам части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С УСТАНОВЛЕННЫМИ В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ.

В результате освоения дисциплины обучающиеся должны демонстрировать следующие результаты.

Наименование компетенций	Индикаторы сформированности компетенций		
	знать	уметь	владеть
Способен к управленческой и инновационно-проектной деятельности в библиотечно-информационной сфере, проведению социологических, психолого-педагогических и маркетинговых исследований (ПК-1)	основные понятия и методы защиты информации	работать с основными методами защиты информации в библиотеке	методами защиты информации в библиотеке

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Структура дисциплины

Очная форма обучения

Общая трудоемкость дисциплины составляет 6 зачетных единицы (216 часов).

№	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по*
				Л	ПЗ	ИЗ	СР	

								семестрам)
1	Раздел I. Концептуальные основы информационной безопасности и защиты информации	5	1-9	16	16		22	Устный опрос, доклады.
2	Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации	5	10-17	16	16		22	Устный опрос, выполнение проекта. Экзамен
3	Раздел III. Организация и документационное обеспечение защиты информации	6	1-10	16	16		4	Устный опрос, доклады.
4	Раздел 4. Правовое обеспечение защиты информации	6	11-17	16	16		4	Письменный опрос. Экзамен
	итого			64	64		52	36

4.2. Тематический план освоения дисциплины по видам учебной деятельности и виды самостоятельной (внеаудиторной) работы

Наименование разделов и тем	***Содержание учебного материала (темы, перечень раскрываемых вопросов): лекции, практические занятия (семинары), индивидуальные занятия, самостоятельная работа обучающихся, курсовая работа***	***Объем часов / з.е.***	***Форми-руемые компе-тенции (по теме)***
1	***2***	***3***	***4***
5-6 семестр			
Раздел I. Концептуальные основы информационной безопасности и защиты информации			
Тема 1.1. Правовое регулирование информационной безопасности и защиты информации	Лекции: Понятия правового регулирования и информационных документов. Федеральный закон "об информации, информатизации и защите информации", законы РФ "о безопасности", "о средствах массовой информации", "о правовой охране программ для ЭВМ и баз данных" и др. Гражданский и уголовный кодексы РФ об ответственности за противоправные действия информационного характера. Указы президента России и постановления	*4*	ПК-1

	информационной безопасности. Государственная система защиты информации. Деятельность федеральных органов государственной власти (федеральной службы безопасности, федерального агентства правительственной связи и информации при президенте РФ государственной технической комиссии при президенте РФ) в сфере информационной безопасности. Система нормативных подзаконных актов по защите информации.		
	Практические занятия (семинары): Компьютерные преступления: классификация, особенности, характерные черты, мотивы, основные виды, способы обнаружения.	*4*	
	Самостоятельная работа Реферат по теме: Лицензирование деятельности и сертификация продуктов и услуг в области защиты информации. Аттестация объектов информатики.	*6*	
Тема 1.2. Угрозы информационной безопасности и противодействие угрозам	Лекции: Понятие угрозы информационной безопасности. Источники угроз, классификация угроз по цели реализации, способу и объекту воздействия. Угрозы информационной безопасности России: виды, внешние и внутренние источники. Угрозы конституционным правам и свободам граждан; угрозы духовной жизни общества; угрозы информационной инфраструктуре и ресурсам. Дестабилизирующие факторы: типы, источники, классификация. Органы добывания информации и основные сферы их интересов. Техническая и агентурная разработка. Легальные и нелегальные способы добывания информации. Условия и методы несанкционированного доступа к добываемой информации. Основные способы дистанционного добывания информации: наблюдение, подслушивание, перехват. Общие принципы добывания и защиты информации. Инженерная защита и техническая охрана объектов. Информационное и энергетическое скрытие. Дезинформирование, маскировка, ослабление сигнала, зашумление.	*4*	ПК-1

	Понятие абсолютной системы защиты.		
	Практические занятия (семинары) Обсуждение тем: Специфические принципы защиты информации. Многозональность и многорубежность защитных мероприятий. Классификация методов защиты информации.	*4*	
	Самостоятельная работа Разработать схему устранения информационных угроз	*6*	
Тема 1.3. Каналы утечки информации	Лекции: Понятие утечки информации, канала утечки технического канала утечки. Особенности утечки информации по сравнению с утечкой материальных объектов. Структура канала передачи информации. Отличия канала утечки от функционального канала; понятие опасного сигнала. Виды источников сигнала, функции передатчика и приемника сигнала, параметры среды распространения. Классификация кадров утечки по физической природе носителя, информативности, структуре, времени появления и действия. Основные показатели, характеризующие каналы утечки. Сравнительная характеристика каналов утечки. Комплексное использование каналов утечки. Оптический канал утечки информации. Особенности и структура оптического канала утечки. Среда распространения, основные виды приемников сигнала. Сравнительная характеристика фотографических, телевизионных изображений в ИК-диапазоне. Противодействие наблюдению в оптическом диапазоне. Способы маскировки и энергетического скрытия объекта защиты. Акустический канал утечки информации. Структура, источники сигналов, среда распространения акустического канала утечки. Характеристики акустических волн как носителей информации, условия их затухания и поглощения. Составные акусто-радиоэлектронный и акусто-оптический каналы, их структура.	*4*	ПК-1

	Способы и средства подслушивания. Классификация закладных устройств. Противодействие подслушиванию. Информационное скрытие: техническое закрытие и шифрование телефонных переговоров, сравнительная характеристика маскираторов, скремблеров и вокодеров. Энергетическое скрытие: звукоизоляция, поглощение акустической волны, акустическое и вибрационное зашумление. Предотвращение несанкционированной записи речевой информации на магнитофон. Обнаружение закладных устройств, определение их принадлежности и подавление. Демаскирующие признаки микрофонных, некамуфлированных и камуфлированных радиозакладок. Основные виды контроля отсутствия закладных устройств. Сущность, порядок осуществления и оборудование для оперативного визуального осмотра. Особенности и сроки проведения профилактического периодического контроля. Проверка помещения после капитального ремонта. Распознавание предметов с подозрением на наличие в них закладок, проверка представительских подарков. Выбор рационального состава средств для контроля помещений. Радиоэлектронный канал утечки информации. Особенности, структура, среда распространения радиоэлектронного канала утечки, основные виды радиоэлектронных каналов. Виды носителей информации и их классификация. Помехи и их классификация по источникам возникновения. Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование источников поля.		
	<u>Практические занятия (семинары)</u> Семинар: - Материально-вещественный канал утечки информации. - Источники и носители информации. - Структура канала. - Способы предотвращения утечки информации.	*4*	

	- Защита информации в отходах деятельности организации. - Защита демаскирующих веществ.		
	Самостоятельная работа Презентация на темы: Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование источников поля.	*6*	
Тема 1.4. Криптографическая защита информации	Лекции: Понятия категории, криптографии, криптоанализа. Главные задачи криптографии и ее отличия от кодирования и стеганографии (тайнописи). Виды криптографических атак. Обобщенная схема криптографической системы и основные варианты ее реализации. Симметричная и ассиметричная криптосистемы. Понятия криптографической защиты, криптографического преобразования, шифра, ключа, имитовставки. Основные характеристики шифров, требования к шифрам, их основные виды. Принципы рассеивания и перемещения как основа современных симметричных криптосистем. Составные шифры, перестановки и подстановки. Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики. Критерии отнесения средств защиты информации к криптографическим. Сравнительная характеристика аппаратных и программных криптографических средств. Функции криптосредств, критически важные для поддержания надежности систем защиты информации. Критерии оценки и выбора криптосредств. Основные режимы шифрования. Архивное шифрование, шифрование при работе в криптографической сети, обработка файлов в интерактивном и пакетном режимах, "прозрачный" режим шифрования. Система ключевой информации. Понятия узла замены, главного, условленного, файлового ключей, ключа пользователя, пароля. Имитовставка: назначение, вычисление и проверка.	*4*	ПК-1

	Проблемы, возникающие при использовании ключей, и пути их решения. Работа в криптографической сети при возможности связи каждого узла сети с любым другим. Понятия сетевой таблицы, ключа сетевой таблицы, сетевого ключа, сетевого набора, ключа сетевого набора. Обмен ключевой информацией между администратором и узлами сети. Организация криптографической сети по схеме "звезда". Действия администратора сети и оператора узла при обмене ключевой информацией. Сравнительный анализ двух схем построения криптографической сети. Общие рекомендации по работе с ключевой информацией.		
	Практические занятия (семинары) Семинар: - Принципы рассеивания и перемещения как основа современных симметричных криптосистем. - Составные шифры, перестановки и подстановки.	*4*	
	Самостоятельная работа Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики.	*4*	
Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации			
Тема 2.1. Защита информации от компьютерных вирусов и других программ с потенциально опасными последствиями	Лекции: Понятие программы с потенциально опасными последствиями, основные функции и виды этих программ. Понятие компьютерного вируса, основные свойства вирусов. Классификация вирусов по среде обитания, алгоритму действия, деструктивным возможностям. Файловые, заголовочные, сетевые, макровирусы. Резидентные вирусы; вирусы, использующие «стелс»-алгоритмы и другие нестандартные приемы. Источники вирусов, основные правила защиты. Антивирусные программы, их типы, сравнительный анализ возможностей, методика использования.	*8*	ПК-1
	Практические занятия (семинары) Семинар: - Программные закладки, их классификация по месту внедрения и применения, основные функции. - Организационно-технические меры	*8*	

	защиты от вирусов и закладок.		
	Самостоятельная работа Тест по теме	*6*	
Тема 2.2. Защита информации в компьютерных сетях	Лекции: Возможности, предоставляемые злоумышленнику общедоступными сетями, и недостатки основных сервисов Интернет с точки зрения информационной безопасности. Межсетевые экраны. Основные требования, предъявляемые к межсетевым экранам, их функции, компоненты межсетевых экранов и их разновидности. Фильтрующие маршрутизаторы, шлюзы сетевого и прикладного уровней. Криптографические маршрутизаторы. Организационные меры обеспечения сетевой информационной безопасности.	*8*	ПК-1
	Практические занятия (семинары) Работа с криптографическими маршрутизаторами.	*8*	
	Самостоятельная работа Реферат по теме	*16*	
Раздел III. Организация и документационное обеспечение защиты информации			
Тема: 3.1. Документация по защите информации	Лекции: Основные виды документов по защите информации: федеральные законы, локальные нормативные акты	*8*	ПК-1
	Практические занятия (семинары) Семинар№1 Правовые аспекты создания и распространения информации. 1.Информация как объект правового регулирования. 2.Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др.	*8*	
	Самостоятельная работа Реферат по теме	*2*	
Тема: 3.2. Система защиты информации	Лекции: Основные способы построения системы защиты информации	*8*	ПК-1
	Практические занятия (семинары) Семинар№2. Информационные ресурсы: классификация	*8*	

	и характеристика их информационных свойств. 1.Основы правового режима информационных ресурсов. Информационные ресурсы как элемент состава имущества и объект права собственности. 2. Государственные информационные ресурсы. Пользование информационными ресурсами. 3. Информационные ресурсы в условиях рыночных отношений.		
	Самостоятельная работа «Стратегия развития информационного общества в Российской Федерации»	*2*	
Раздел IV. Правовое обеспечение защиты информации			
Тема: 4.1. Основные правовые документы защиты информации	Лекции: Основные правовые документы, касающиеся защиты информации	*8*	ПК-1
	Практические занятия (семинары) Семинар№3, №4 Защита информации и прав субъектов в области информационных процессов и информатизации 1. Защита информации и ее цели. 2. Характеристика основных методов и средств защиты информации. 3. Права и обязанности субъектов в области защиты информации. 4. Защита прав субъектов в сфере информационных процессов и информатизации. 5. Защита прав на доступ к информации.	*8*	
	Самостоятельная работа Закон «О персональных данных»	*2*	
Тема: 4.2. Управление процессом защиты информации	Лекции: Основные процессы управления защитой информации	*8*	ПК-1
	Практические занятия (семинары) Семинар№5,6 Интеллектуальная собственность, как объект правовой охраны. 1.Понятие интеллектуальной собственности и система ее правовой охраны. 2.Основные институты права интеллектуальной собственности. 3.Система Российского законодательства об интеллектуальной собственности. 4.История развития Российского	*8*	

	законодательства об охране интеллектуальной собственности..		
	Самостоятельная работа Итоговый тест по дисциплине	*2*	
Примерная тематика курсовой работы *(если предусмотрено)*			
Самостоятельная работа обучающихся над курсовой работой *(если предусмотрено)*			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)		*Экзамен (36)*	
	ВСЕГО:	*216*	

Заочная форма обучения

Общая трудоемкость дисциплины составляет 6 зачетных единицы (216 часов).

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ИЗ	СР	
1	Раздел I. Концептуальные основы информационной безопасности и защиты информации	5	1-9	2	6		40	Устный опрос, доклады.
2	Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации	5	10-17	4	6		38	Устный опрос, выполнение проекта. Экзамен
3	Раздел III. Организация и документационное обеспечение защиты информации	6	1-10	2	6		30	Устный опрос, доклады.
4	Раздел 4. Правовое обеспечение защиты информации	6	11-17	4			39	Письменный опрос. Экзамен
	итого			12	24		147	Контроль - 9 Консультации - 24

4.2. Тематический план освоения дисциплины по видам учебной деятельности и виды самостоятельной (внеаудиторной) работы

Наименование разделов и тем	***Содержание учебного материала (темы, перечень раскрываемых вопросов): лекции, практические занятия (семинары), индивидуальные занятия, самостоятельная работа обучающихся, курсовая работа***	***Объем часов / з.е.***	***Форми-руемые компе-тенции (по теме)***
1	***2***	***3***	***4***
5-6 семестр			
Раздел I. Концептуальные основы информационной безопасности и защиты информации			
Тема 1.1. Правовое регулирование информационной безопасности и защиты информации	Лекции: Понятия правового регулирования и информационных документов. Федеральный закон "об информации, информатизации и защите информации", законы РФ "о безопасности", "о средствах массовой информации", "о правовой охране программ для ЭВМ и баз данных" и др. Гражданский и уголовный кодексы РФ об ответственности за противоправные действия информационного характера. Указы президента России и постановления информационной безопасности. Государственная система защиты информации. Деятельность федеральных органов государственной власти (федеральной службы безопасности, федерального агентства правительственной связи и информации при президенте РФ государственной технической комиссии при президенте РФ) в сфере информационной безопасности. Система нормативных подзаконных актов по защите информации.	*2*	ПК-1
	Практические занятия (семинары): Компьютерные преступления: классификация, особенности, характерные черты, мотивы, основные виды, способы обнаружения.	*2*	
	Самостоятельная работ Реферат по теме: Лицензирование деятельности и сертификация продуктов и услуг в области защиты информации. Аттестация объектов информатики.	*10*	
Тема 1.2. Угрозы информационной безопасности и противодействие угрозам	Лекции: Понятие угрозы информационной безопасности. Источники угроз, классификация угроз по цели реализации,		ПК-1

	способу и объекту воздействия. Угрозы информационной безопасности России: виды, внешние и внутренние источники. Угрозы конституционным правам и свободам граждан; угрозы духовной жизни общества; угрозы информационной инфраструктуре и ресурсам. Дестабилизирующие факторы: типы, источники, классификация. Органы добывания информации и основные сферы их интересов. Техническая и агентурная разработка. Легальные и нелегальные способы добывания информации. Условия и методы несанкционированного доступа к добываемой информации. Основные способы дистанционного добывания информации: наблюдение, подслушивание, перехват. Общие принципы добывания и защиты информации. Инженерная защита и техническая охрана объектов. Информационное и энергетическое скрытие. Дезинформирование, маскировка, ослабление сигнала, зашумление. Понятие абсолютной системы защиты.		
	<u>Практические занятия (семинары)</u> Обсуждение тем: Специфические принципы защиты информации. Многозональность и многорубежность защитных мероприятий. Классификация методов защиты информации.	*2*	
	<u>Самостоятельная работа</u> Разработать схему устранения информационных угроз	*10*	
Тема 1.3. Каналы утечки информации	<u>Лекции:</u> Понятие утечки информации, канала утечки технического канала утечки. Особенности утечки информации по сравнению с утечкой материальных объектов. Структура канала передачи информации. Отличия канала утечки от функционального канала; понятие опасного сигнала. Виды источников сигнала, функции передатчика и приемника сигнала, параметры среды распространения. Классификация кадров утечки по физической природе носителя,		ПК-1

	информативности, структуре, времени появления и действия. Основные показатели, характеризующие каналы утечки. Сравнительная характеристика каналов утечки. Комплексное использование каналов утечки. Оптический канал утечки информации. Особенности и структура оптического канала утечки. Среда распространения, основные виды приемников сигнала. Сравнительная характеристика фотографических, телевизионных изображений в ИК-диапазоне. Противодействие наблюдению в оптическом диапазоне. Способы маскировки и энергетического скрытия объекта защиты. Акустический канал утечки информации. Структура, источники сигналов, среда распространения акустического канала утечки. Характеристики акустических волн как носителей информации, условия их затухания и поглощения. Составные акусто-радиоэлектронный и акусто-оптический каналы, их структура. Способы и средства подслушивания. Классификация закладных устройств. Противодействие подслушиванию. Информационное скрытие: техническое закрытие и шифрование телефонных переговоров, сравнительная характеристика маскираторов, скремблеров и вокодеров. Энергетическое скрытие: звукоизоляция, поглощение акустической волны, акустическое и вибрационное зашумление. Предотвращение несанкционированной записи речевой информации на магнитофон. Обнаружение закладных устройств, определение их принадлежности и подавление. Демаскирующие признаки микрофонных, некамуфлированных и камуфлированных радиозакладок. Основные виды контроля отсутствия закладных устройств. Сущность, порядок осуществления и оборудование для оперативного визуального осмотра. Особенности и сроки проведения профилактического периодического		

	контроля. Проверка помещения после капитального ремонта. Распознавание предметов с подозрением на наличие в них закладок, проверка представительских подарков. Выбор рационального состава средств для контроля помещений. Радиоэлектронный канал утечки информации. Особенности, структура, среда распространения радиоэлектронного канала утечки, основные виды радиоэлектронных каналов. Виды носителей информации и их классификация. Помехи и их классификация по источникам возникновения. Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование источников поля.		
	<u>Практические занятия (семинары)</u> Семинар: - Материально-вещественный канал утечки информации. - Источники и носители информации. -Структура канала. - Способы предотвращения утечки информации. - Защита информации в отходах деятельности организации. - Защита демаскирующих веществ.	*2*	
	<u>Самостоятельная работа</u> Презентация на темы: Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование источников поля.	*10*	
Тема 1.4. Криптографическая защита информации	<u>Лекции:</u> Понятия категории, криптографии, криптоанализа. Главные задачи криптографии и ее отличия от кодирования и стеганографии (тайнописи). Виды криптографических атак. Обобщенная схема криптографической системы и основные варианты ее реализации. Симметричная и ассиметричная криптосистемы. Понятия криптографической защиты, криптографического преобразования, шифра, ключа, имитовставки. Основные характеристики шифров, требования к		ПК-1

	шифрам, их основные виды. Принципы рассеивания и перемещения как основа современных симметричных криптосистем. Составные шифры, перестановки и подстановки. Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики. Критерии отнесения средств защиты информации к криптографическим. Сравнительная характеристика аппаратных и программных криптографических средств. Функции криптосредств, критически важные для поддержания надежности систем защиты информации. Критерии оценки и выбора криптосредств. Основные режимы шифрования. Архивное шифрование, шифрование при работе в криптографической сети, обработка файлов в интерактивном и пакетном режимах, "прозрачный" режим шифрования. Система ключевой информации. Понятия узла замены, главного, условленного, файлового ключей, ключа пользователя, пароля. Имитовставка: назначение, вычисление и проверка. Проблемы, возникающие при использовании ключей, и пути их решения. Работа в криптографической сети при возможности связи каждого узла сети с любым другим. Понятия сетевой таблицы, ключа сетевой таблицы, сетевого ключа, сетевого набора, ключа сетевого набора. Обмен ключевой информацией между администратором и узлами сети. Организация криптографической сети по схеме "звезда". Действия администратора сети и оператора узла при обмене ключевой информацией. Сравнительный анализ двух схем построения криптографической сети. Общие рекомендации по работе с ключевой информацией.		
	<u>Практические занятия (семинары)</u> Семинар: - Принципы рассеивания и перемещения как основа современных симметричных криптосистем. - Составные шифры, перестановки и подстановки.		

	Самостоятельная работа Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики.	*10*	
Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации			
Тема 2.1. Защита информации от компьютерных вирусов и других программ с потенциально опасными последствиями	Лекции: Понятие программы с потенциально опасными последствиями, основные функции и виды этих программ. Понятие компьютерного вируса, основные свойства вирусов. Классификация вирусов по среде обитания, алгоритму действия, деструктивным возможностям. Файловые, заголовочные, сетевые, макровирусы. Резидентные вирусы; вирусы, использующие "стелс"-алгоритмы и другие нестандартные приемы. Источники вирусов, основные правила защиты. Антивирусные программы, их типы, сравнительный анализ возможностей, методика использования.	*2*	ПК-1
	Практические занятия (семинары) Семинар: - Программные закладки, их классификация по месту внедрения и применения, основные функции. - Организационно-технические меры защиты от вирусов и закладок.	*2*	
	Самостоятельная работа Тест по теме	*18*	
Тема 2.2. Защита информации в компьютерных сетях	Лекции: Возможности, предоставляемые злоумышленнику общедоступными сетями, и недостатки основных сервисов Интернет с точки зрения информационной безопасности. Межсетевые экраны. Основные требования, предъявляемые к межсетевым экранам, их функции, компоненты межсетевых экранов и их разновидности. Фильтрующие маршрутизаторы, шлюзы сетевого и прикладного уровней. Криптографические маршрутизаторы. Организационные меры обеспечения сетевой информационной безопасности.	*2*	ПК-1
	Практические занятия (семинары) Работа с криптографическими маршрутизаторами.	*4*	
	Самостоятельная работа	*20*	

	Реферат по теме		
Раздел III. Организация и документационное обеспечение защиты информации			
Тема: 3.1. Документация по защите информации	Лекции: Основные виды документов по защите информации: федеральные законы, локальные нормативные акты	*2*	ПК-1
	Практические занятия (семинары) Семинар№1 Правовые аспекты создания и распространения информации. 1.Информация как объект правового регулирования. 2.Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др.	*4*	
	Самостоятельная работа Реферат по теме	*10*	
Тема: 3.2. Система защиты информации	Лекции: Основные способы построения системы защиты информации		ПК-1
	Практические занятия (семинары) Семинар№2. Информационные ресурсы: классификация и характеристика их информационных свойств. 1.Основы правового режима информационных ресурсов. Информационные ресурсы как элемент состава имущества и объект права собственности. 2. Государственные информационные ресурсы. Пользование информационными ресурсами. 3. Информационные ресурсы в условиях рыночных отношений.	*2*	
	Самостоятельная работа «Стратегия развития информационного общества в Российской Федерации»	*20*	
Раздел IV. Правовое обеспечение защиты информации			
Тема: 4.1. Основные правовые документы защиты информации	Лекции: Основные правовые документы, касающиеся защиты информации	*2*	ПК-1
	Практические занятия (семинары) Семинар№3, №4 Защита информации и прав субъектов в области информационных процессов и		

	информатизации 1. Защита информации и ее цели. 2. Характеристика основных методов и средств защиты информации. 3. Права и обязанности субъектов в области защиты информации. 4. Защита прав субъектов в сфере информационных процессов и информатизации. 5. Защита прав на доступ к информации.		
	Самостоятельная работа Закон «О персональных данных»	*20*	
Тема: 4.2. Управление процессом защиты информации	Лекции: Основные процессы управления защитой информации	*2*	ПК-1
	Практические занятия (семинары) Семинар№5,6 Интеллектуальная собственность, как объект правовой охраны. 1.Понятие интеллектуальной собственности и система ее правовой охраны. 2.Основные институты права интеллектуальной собственности. 3.Система Российского законодательства об интеллектуальной собственности. 4.История развития Российского законодательства об охране интеллектуальной собственности.		
	Самостоятельная работа Итоговый тест по дисциплине	*19*	
Примерная тематика курсовой работы *(если предусмотрено)*			
Самостоятельная работа обучающихся над курсовой работой *(если предусмотрено)*			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)		*Экзамен (36)*	
	ВСЕГО:	*216*	

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Номер п/п	***Наименование раздела***	***Используемые образовательные технологии***
1	***2***	***5***
1	***Раздел 1 Концептуальные основы информационной безопасности и защиты информации***	Индивидуальная работа студента с лекциями и учебной литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). Дискуссия: «Что такое защита информации и для чего ее необходимо изучать?».

2	***Раздел 2 Защита информации от несанкционированного доступа и разграничение доступа к информации***	Индивидуальная работа студента с первоисточниками и литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). Тестирование студентов по разделу дисциплины
3	***Раздел 3 Организация и документационное обеспечение защиты информации***	Индивидуальная работа студента с первоисточниками и литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов).
4	***Раздел 4 Правовое обеспечение защиты информации***	Индивидуальная работа студента с первоисточниками и литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). Тестирование студентов по разделу дисциплины Дискуссия: «Основные виды документов по защите информации».

6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6.1. Контроль освоения дисциплины

Контроль освоения дисциплины производится в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации студентов ФГБОУ ВО «Краснодарский государственный институт культуры». Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля.

Текущий контроль успеваемости студентов по дисциплине производится в следующих формах:

- *устный опрос*
- *письменные индивидуальные задания*

Рубежный контроль предусматривает оценку знаний, умений и навыков студентов по пройденному материалу по данной дисциплине на основе текущих оценок, полученных ими на занятиях за все виды работ. В ходе рубежного контроля используются следующие методы оценки знаний:

устные ответы,
письменные работы,
практические и лабораторные работы,
оценка выполнения самостоятельной работы студентов:
реферативная работа,

Промежуточный контроль по результатам семестра по дисциплине проходит в форме экзамена.

6.2. Оценочные средства

6.2.1. Примеры тестовых заданий (ситуаций)

Вопросы для контроля знаний студентов (тесты)

1. Цель защиты информации:

а) предотвращение утечки, хищения, утраты, искажения, подделки информации;

б) предотвращения угроз безопасности личности, общества, государства;

в) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

г) защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных имеющихся в информационных системах;

д) сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

е) защита прав и свобод в условиях новой политической системы;

ж) предотвращение создания новых технологий в сфере защиты информации.

2.В отношении чего устанавливается режим защиты информации:

а) в отношении сведений, отнесенных к государственной тайне;

б) в отношении библиографических сведений;

в) в отношении конфиденциальной документационной информации;

г) в отношении информации по безопасности жизнедеятельности;

д) в отношении персональных данных федеральным законом.

3.Объекты авторского права:

а) литературные произведения;

б) музыкальные произведения с текстом и без него;

в) произведения архитектуры, градостроительства и садово-паркового искусства;

г) информационные ресурсы;

д) государственные символы и знаки;

е) произведения народного творчества.

4.В каком документе закреплен правовой статус информации:

а) закон РФ «О библиотечном деле»;

б) закон РФ «Об авторском праве»;

г) закон РФ «Об информации, информатизации и защите информации».

5.Срок действия авторского права:

а) в течение всей жизни автора и 25 лет после его жизни;

б) в течение всей жизни автора и 50 лет после его жизни;

в) в течение всей жизни автора и 100 лет после его жизни.

6.Субъекты смежных прав:

а) исполнители;

б) авторы;

в) производители фонограмм;

г) организации эфирного или кабельного вещания.

7. Объективная форма представления и организации совокупности

данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ):

а) информационная система;

б) база данных;

в) информационные ресурсы.

8. Факсимильное воспроизведение в любых размерах и форме одного или более экземпляров оригиналов или копий письменных и других графических произведений путем фотокопирования или с помощью других технических средств, иных, чем издания:

а) репродуцирование;

б) тиражирование;

в) дублирование.

9. Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах):

а) информационные процессы;

б) информационные процессы;

в) информация.

10. Показывать, исполнять, передавать в эфир или совершать иное действие (за исключением распространения экземпляров произведения или фонограммы), посредством которого произведения, фонограммы, исполнения, постановки, передачи организации эфирного или кабельного вещания становится доступным для слухового и (или) зрительного восприятия, независимо от их фактического восприятия публикой:

а) публичный показ;

б) сообщать;

в) сообщения для всеобщего сведения.

11.Когда был опубликован и начал действовать закон РФ «Об информации, информатизации и защите информации»?

а)1989г.

б)1997г.

в)1993г.

г)1995г.

Определите понятие:

12. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления:

а) документ;

б) информация;

в) информационные ресурсы.

13. Любая исключительно звуковая запись исполнений или иных звуков:

а) запись;

б) произведения;

в) фонограмма.

14. Выпуск в обращение экземпляров произведения, произведение фонограммы в количестве, достаточном для удовлетворения разумных потребностей публики исходя из характера произведения, фонограммы:

а) воспроизведение произведения;

б) опубликование;

в) обнародования произведения.

15. Организационно-упорядоченная совокупность документов (массив документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы:

а) информатизация;

б) информационная система;

в) база данных.

16. Субъект в полном объеме реализующей полномочия владения, пользования, распоряжения указанными объектами:

а) собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения;

б) владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения;

в) пользователь информацией.

17. Демонстрация оригинала или экземпляра произведения непосредственно или на экране с помощью пленки, диапозитива, телевизионного кадра или иных технических средств, а также демонстрация отдельных кадров аудиовизуального произведения без соблюдения их последовательности:

а) передача в эфир;

б) показ произведения;

в) репродуцирование.

18. Физическое или юридическое лицо, взявшее на себя инициативу и ответственность за изготовление такого произведения; при отсутствии доказательств иного изготовителя аудиовизуального произведения признается физическое или юридическое лицо, имя или наименование которого обозначено на этом произведении обычным путем:

а) изготовитель фонограммы;

б) изготовитель аудиовизуального произведения;

в) изготовитель декоративно – прикладного искусства.

19. Зафиксированная на материальном носителе информация с реквизитами, позволяющая ее идентифицировать:

а) информация;

б) документ;

в) база данных.

20. Представление произведений, фонограмм, исполнений, постановок посредством игры, декламация, пение, танца в живом исполнении или с помощью технических средств; показ кадров аудиовизуального произведения

в их последовательности (с сопровождением или без сопровождения звуком):

а) передача в эфир;

б) исполнение;

в) публичный показ.

21. Осуществленное с согласия автора действие, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, передачи в эфир или иным способом:

а) показ произведения;

б) обнародования произведения;

в) исполнение.

22. Субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом:

а) владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения;

б) собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения;

в) автор.

23. Копия произведения, изготовленная в любой материальной форме:

а) экземпляр произведения;

б) экземпляр фонограммы.

6.2.2. Контрольные вопросы для проведения текущего контроля

1.Информация как объект правового регулирования.

2.Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др.

3.Основы правового режима информационных ресурсов. Информационные ресурсы как элемент состава имущества и объект права собственности.

4.Государственные информационные ресурсы. Пользование информационными ресурсами.

5.Информационные ресурсы в условиях рыночных отношений.

6. Защита информации и ее цели.

7. Характеристика основных методов и средств защиты информации.

8. Права и обязанности субъектов в области защиты информации.

9. Защита прав субъектов в сфере информационных процессов и информатизации.

10. Защита прав на доступ к информации.

11.Понятие интеллектуальной собственности и система ее правовой охраны.

12.Основные институты права интеллектуальной собственности.

13.Система Российского законодательства об интеллектуальной собственности.

14.История развития Российского законодательства об охране интеллектуальной собственности.

15. Объекты авторского права.

16. Субъекты авторского права.

17. Права авторов произведений науки, литературы и искусства.

18. Авторский договор.

19. Защита авторских прав.

6.2.3. Тематика эссе, рефератов, презентаций

1. Теоретические основы защиты информации
2. Информационные ресурсы как объект права
3. Защита информации в автоматизированных системах обработки данных
4. Конфиденциальное делопроизводство
5. Деятельность национальных институтов Российской Федерации в области информационной безопасности
6. Информационная безопасность человека и общества
7. Концептуальная модель информационной безопасности
8. Основные функции системы обеспечения информационной безопасности Российской Федерации и элементы ее организационной основы
9. Общие методы обеспечения информационной безопасности Российской Федерации
10. Источники угроз информационной безопасности Российской Федерации
11. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни
12. Методология обеспечения информационной безопасности деятельности общества
13. Эволюция подходов к обеспечению информационной безопасности
14. Области и объекты по обеспечению ИБ и защите информационной деятельности
15. Объекты защиты информационной деятельности и обеспечения ИБ
16. Стратегии обеспечения ИБ фирм
17. Организационно-правовое обеспечение ИБ
18. Отечественные и международные нормативно-правовые акты обеспечение ИБ
19. Аудит информационной безопасности
20. Организационно-технические аспекты защиты информации

6.2.4. Вопросы к зачету по дисциплине (не предусмотрено по плану)

6.2.5. Вопросы к экзамену по дисциплине

1. Доктрина ИБ РФ – определение, принципы.
2. Основные эволюционные подходы к обеспечению ИБ деятельности общества вы знаете.
3. Российской Федерации в информационной сфере.
4. Информационное оружие - определение.
5. Информационная безопасность РФ – определение, основные понятия.
6. Криптографическая защита информации.
7. Сформулируйте интересы государства, общества и личности в информационной сфере.
8. Цифровая подпись.
9. Охарактеризуйте 2 основных рода информации, используемых при функционировании социальных, технических и организационно-технических систем.
10. Перечислите внешние источники угроз ИБ РФ.
11. Доступ к информации (несанкционированный доступ).
12. Персональные данные – определение.
13. Понятие информация, ее ценность для владельца.
14. Политика безопасности - определение.
15. Конфиденциальная информация, государственная и коммерческая тайна.
16. Каналы утечки информации.
17. Три степени секретности информации.
18. Государственная тайна.
19. Три категории ценности коммерческой информации.
20. Защита информации от компьютерных вирусов.
21. Товарная ценность информации, пути ее получения.
22. Коммерческая тайна.
23. Основные методы определения объема информации.
24. Конфиденциальная информация.
25. Основные виды угроз ИБ РФ.
26. Правовые аспекты создания информации.
27. Четыре основных принципа обеспечения ИБ РФ.
28. Защита информации в компьютерных сетях.
29. Основные направления международного сотрудничества Российской Федерации в области ИБ.
30. Внутренние источники угроз ИБ РФ.
31. Правовые аспекты распространения информации.

32. Интеллектуальная собственность – объект правовой охраны.
33. Авторское право.
34. Основные функции системы обеспечения ИБ РФ.
35. Источники права на доступ к информации.
36. Технология защиты документной информации.
37. Комплексное обеспечение ИБ РФ.
38. Аудит информационной безопасности.
39. Информационные ресурсы как объект права.
40. Конфиденциальное делопроизводство.
41. Особенности обеспечения информационной безопасности РФ в различных сферах общественной жизни.
42. Специфические принципы защиты информации в компьютерных сетях.

6.2.6. Примерная тематика курсовых работ

Не предусмотрено

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

7.1. Основная литература

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов ; Межрегион. акад. безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения: 15.07.2019). – Текст : электронный.
2. Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. – Ростов-на-Дону : Феникс, 2017. – 349 с. – (Высшее образование). – Текст : непосредственный.
3. Родичев, Ю. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для студентов вузов / Ю. Родичев. – Москва ; Санкт-Петербург : Питер, 2008. – 272 с. – (Учебное пособие). – Текст : непосредственный.
4. Алешин, Л. И. Безопасность в библиотеке : учебно-методическое пособие. Вып. 18 / Л. И. Алешин. – Москва : Либерея-Бибинформ, 2005. – 247 с. – (Библиотекарь и время. XXI век). – Текст : непосредственный.

7.2. Дополнительная литература

1. Фефилов, А. Д. Методы и средства защиты информации в сетях : практическое пособие / А. Д. Фефилов. – Москва : Лаборатория книги, 2011. – 105 с. – Режим доступа: по подписке. – URL:

http://biblioclub.ru/index.php?page=book&id=140796 (дата обращения: 15.07.2019). – Текст : электронный.
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров ; С.-Петерб. политехн. ун-т Петра Великого. – Москва : Юрайт, 2017. – 321 с. – (Университеты России). – Текст : непосредственный.
3. Мельников, В. П. Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева ; под ред. В. П. Мельникова. – 2-е изд., перераб. и доп. – Москва : Кнорус, 2018. – 371 с. – (Бакалавриат). – Текст : непосредственный.
4. Организационно-правовое обеспечение информационной безопасности : учебное пособие для студентов вузов / под ред. А. А. Стрельцова. – Москва : Академия, 2008. – 256 с. – (Высшее профессиональное образование). – Текст : непосредственный.

7.3. Периодические издания

1. Библиотековедение
2. Научные и технические библиотеки
3. Научно-техническая информация (НТИ). Серия 1. Организация и методика информационной работы
4. Современная библиотека
5. Школьная библиотека
6. Университетская книга (ЭБС «УБО»)

7.4. Интернет-ресурсы

http://otherreferats.allbest.ru/marketing/00068136_0.html учебники http://mirknig.com/ - теоретические и практические пособия

7.5. Методические указания и материалы по видам занятий

Представление учебного материала целесообразно посредством оптимального сочетания традиционных (проблемные лекции, тематические семинарские и практические занятия) и активных (деловые и ролевые игры, разбор конкретных ситуаций, многоплановые ситуационные задачи, тренинги, «мозговые штурмы», дискуссии, индивидуальные и коллективные задания поисково – исследовательского характера и др.) форм обучения.

В качестве промежуточных средств оценки усвоения курса возможно применение тестового контроля (тематические и аналитические тесты, тестовые задания) в традиционной и компьютерной формах.

7.6. Программное обеспечение

Программное обеспечение и информационно-справочные системы:

- Microsoft™ Windows Professional 7 (госконтракт 08/ОАЭФ/11 договор Tr047534) сертификат 49178087
- Microsoft™ Office® 2007 Лицензия номер 43108483)

- Kaspersky Endpoint Security (сублицензионный договор 316 от 12.09.2017)
- Adobe Flash Player ActiveX (Free)
- Adobe Reader(Free)
- Google Chrom (Free)
- Teach infiniti Pro (в комплекте с досками)

SMART Learning Suite, 1 year subscription

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Преподавание дисциплины в вузе обеспечено наличием аудиторий (в том числе оборудованных проекционной техникой) для всех видов занятий.

Действуют компьютерные классы с лицензионным программным обеспечением. Имеются рабочие места с выходом в Интернет для самостоятельной работы.

Все компьютерные классы подключены к локальной сети вуза и имеют выход в интернет, в наличии стационарное мультимедийное оборудование (проектор+ экран), возможно проведение занятий на базе музея вуза (тачпанель, экран, проектор).

Обучающиеся пользуются

- вузовской библиотекой с электронным читальным залом;

- учебниками и учебными пособиями;

- аудио и видео материалами.

Все помещения соответствуют требованиям санитарного и противопожарного надзора.

Дополнения и изменения
к рабочей программе учебной дисциплины (модуля)
Защита информации и информационная безопасность
на 20__-20__ уч. год

В рабочую программу учебной дисциплины вносятся следующие изменения:

- _____;
- _____;

- _____.
- _____;
- _____;
- _____.

Дополнения и изменения к рабочей программе рассмотрены и рекомендованы на заседании кафедры ББД
(наименование)

Исполнитель(и):

_____/_____/_____/_____
(должность) (подпись) (Ф.И.О.) (дата)

_____/_____/_____/_____
(должность) (подпись) (Ф.И.О.) (дата)

Заведующий кафедрой

_____/_____/_____/_____
(наименование кафедры) (подпись) (Ф.И.О.) (дата)