Министерство культуры Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Северо-Кавказский государственный институт искусств»

Колледж культуры и искусств

«Утверждаю»
проректор по учебной работе
Б.Г.Ашхотов
18 февраля 2015 г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ
МДК.04. 02
Информационная безопасность
для специальности
51.02.03 Библиотековедение

Нальчик, 2015г.

Рабочая программа по дисциплине «Информационная безопасность» составлена на основе Федерального государственного Образовательного стандарта по специальности 51.02.03 Библиотековедение углубленной подготовки

Одобрена предметно—цикловой комиссией «Библиотековедение»
Протокол № 4
От « 16» февраля 2015 г.
Председатель ПЦК «Библиотековедение» / Прокудина Н.П.

Разработчик : Прокудина Н.П., преподаватели ККИ СКГИИ

Эксперт: Гегиева Л.Х., преподаватели ККИ СКГИИ

Содержание:

Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате изучения обязательной части цикла обучающийся должен:

уметь:

- определять необходимый уровень безопасности информации;
- правильно организовать мероприятия по защите информации;
- применять в профессиональной деятельности нормативно-правовую базу информационной безопасности.

знать:

- основные понятия, объекты, цели и задачи защиты информации;
- угрозы информационной безопасности – их классификацию и источники возникновения.
- приемы защиты информации; виды и характеристики современных средств защиты.
- классификацию и характеристику компьютерных вирусов;
- общую характеристику средств нейтрализации компьютерных вирусов.
- нормативно-правовую базу информационной безопасности.

2.Требования к уровню освоения содержания дисциплины.

В процессе освоения данной дисциплины студент формирует следующие компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования

профессиональной деятельности.

ОК 6. Работать в коллективе, обеспечивать его сплочение, эффективно общаться с коллегами,руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 4.1. Использовать современные информационные и телекоммуникационные технологии в профессиональной деятельности.

ПК 4.2. Использовать прикладное программное обеспечение в формировании библиотечных фондов.

ПК 4.3. Создавать и использовать базы данных в профессиональной деятельности.

ПК 4.4. Использовать информационные ресурсы и авторитетные файлы корпоративных информационных систем.

ПК 4.5. Использовать программные средства повышения информационной безопасности.

В результате освоения дисциплины обучающийся должен уметь:

использовать средства автоматизации и компьютеризации отдельных участков и процессов библиотечно-библиографической деятельности;

программное обеспечение библиотечных процессов;

применять компьютерную технику и телекоммуникативные средства в

процессе библиотечно-библиографической деятельности;

применять мультимедийные технологии;

оценивать результативность различных этапов информатизации библиотеки;

анализировать деятельность отдельных подсистем АБИС и формулировать требования к их дальнейшему развитию;

вести прием и передачу сообщений по электронной почте;

использовать "Adobe Photoshop", "ABBYY Fine Reader", "Microsoft Publisher" и "Microsoft Point";

печатать публикации на принтере; работать с электронными документами;

обеспечивать надежное хранение документов и данных;

использовать внешние базы данных и корпоративных ресурсов библиотечно-информационных систем;

знать:

основные стратегические направления развития библиотек на современном этапе;

состав, функции и возможности информационных и телекоммуникативных технологий;

классификацию, установку и сопровождение программного обеспечения, типы компьютерных сетей;

принципы использования мультимедиа;

основные свойства и характеристики АБИС;

виды и правила сетевого взаимодействия;

особенности функционирования различных видов автоматизированных рабочих мест;

виды информационных ресурсов,

Интернет-ресурсы и услуги;

виды электронных документов и баз

данных;

принципы разработки web-документов;

безопасность работы в сети Интернет.

3.Объём дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	***63***
Обязательная аудиторная учебная нагрузка (всего)	***42***
в том числе:	
лабораторные занятия	
практические занятия	
контрольные работы	
Самостоятельная работа обучающегося (всего)	***21***
формы контроля конт. раб.- 7семестр, зачёт - 8 семестр	

4.Содержание дисциплины и требования к формам и содержанию текущего, промежуточного, итогового контроля (программный минимум, зачетно- экзаменационные требования).

Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов
1	*2*		*3*
Раздел 1. Борьба с угрозами несанкционированного доступа			**15**
Тема 1.1 Актуальность проблемы обеспечения информационной безопасности	**Содержание учебного материала**		4
	1	Основные понятия объекты, цели и задачи информационной безопасности**.** Основные понятия информационной безопасности.	
	2	Угрозы информационной безопасности: классификация, источники возникновения	
	Практические занятия		1
	1	Составление схемы информационных потоков на исследуемом объекте.	
	Самостоятельная работа обучающегося.		2
	Рассмотреть действия и события, нарушающие информационную безопасность		
Тема 1.2 Виды мер обеспечения информационной безопасности	**Содержание учебного материала**		8
	1	Виды мер обеспечения информационной безопасности.	
	2	Мероприятия по защите информации.	
	3	Виды и характеристики современных средств защиты.	
	4	Аспекты, относящиеся к средствам защиты: аппаратные ключи, лицензирование, метод авторизации	
	Практические занятия		2
	1	Определение первоочередных мероприятий по обеспечению информационной безопасности.	
	2	Оценка первоочередных мероприятий по обеспечению информационной безопасности.	
	Самостоятельная работа обучающегося		2
	Подготовить презентацию на тему “Современные технические средства защиты информации” Рассмотреть необходимые мероприятия по обеспечению информационной безопасности		
Раздел 2. Борьба с вирусным заражением			**13**
Тема 2.1 Проблема вирусного заражения и структура современных вирусов	**Содержание учебного материала:**		8
	1	Общая характеристика компьютерных вирусов. Классификация компьютерных вирусов.	
	2	Признаки проявления вирусов. Структура вирусов, пути их распространения.	
	3	Кейлоггеры. Классификация по типу, по месту хранения, по методу отправки и методу применения.	
	4	Модели поведения вирусов и их деструктивные действия	
	Практические занятия:		1
	1	Виды и особенности компьютерных вирусов	
	Самостоятельная работа обучающегося		2

	Подготовить презентацию на тему “Компьютерный вирус ”		
Тема 2.2 Защита от воздействия вирусов	**Содержание учебного материала:**		4
	1	Классификация методов защиты от компьютерных вирусов. Виды и назначение антивирусных программ	
	2	Состав программного комплекса защиты от вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.	
	Практические работы		2
	1	Обзор современных антивирусных программ	
	Самостоятельная работа обучающегося		2
	Подготовить презентацию на тему “Антивирусная программа ”		
Раздел 3. Организационно-правовое обеспечение информационной безопасности			**4**
Тема 3.1 Международные, российские и отраслевые правовые документы	**Содержание учебного материала:**		4
	1	История становления Российского законодательства в области информационной безопасности, основные нормативные акты.	
	2	Международные правовые акты по защите информации.	
	Практические работы		2
	1	Нормативно-правовая база информационной безопасности	
	Самостоятельная работа обучающегося		2
	Изучить нормативно-правовую базу РФ и статьи Уголовного кодекса РФ, регулирующие вопросы информационной безопасности		
	Всего: Занятия на уроках в том числе практические занятия самостоятельная работа		**42** **22** **10** **10**

Контроль и оценка результатов освоения учебной дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения устных и письменных опросов, практических занятий, а также выполнения обучающимися индивидуальных заданий, самостоятельной работы

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1	*2*
Умения:	
- определять необходимый уровень безопасности информации;	практические работы, индивидуальные задания, устный опрос, письменный опрос.
- правильно организовать мероприятия по защите информации;	практические работы, индивидуальные задания, устный опрос, письменный опрос.
- применять в профессиональной деятельности нормативно-правовую базу информационной безопасности.	практические работы, индивидуальные задания, устный опрос, письменный опрос.
Знания:	
- основные понятия, объекты, цели и задачи защиты информации;	индивидуальные задания, устный опрос, письменный опрос.
- угрозы информационной безопасности – их классификацию и источники возникновения.	индивидуальные задания, устный опрос, письменный опрос.
- приемы защиты информации; виды и характеристики современных средств защиты.	индивидуальные задания, устный опрос, письменный опрос.
- классификацию и характеристику компьютерных вирусов;	индивидуальные задания, устный опрос.
- общую характеристику средств нейтрализации компьютерных вирусов.	индивидуальные задания, устный опрос.
- нормативно-правовую базу информационной безопасности	индивидуальные задания, письменный опрос.

5.Учебно-методическое и информационное обеспечение дисциплины.

Средства обучения

1. ОС Windows 2000 и выше, либо XP;
2. MS Office 2000 и выше;

3. AVP
4. DrWeb;
5. Borland TASM 5,0
6. Turbo Pascal 7
7. Borland Delphi 7
8. Borland C++
9. Электронные пакеты программ «Защита от хакеров», «Все для безопасности вашего компьютера, «Безопасность сети 2005»
10. Программный комплекс «Криптоцентр».

Перечень рекомендуемых учебных изданий, дополнительной литературы

ОСНОВНЫЕ ИСТОЧНИКИ

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность учебное пособие для студентов учреждений среднего профессионального образования – М.: ИД «Академия», 2010 г. -336 с.
2. В.Ф. Шаньгин Информационная безопасность компьютерных систем и сетей: учебное пособие – М.: ИД «ФОРУМ», 2010 г.- 416 с.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ

1. Партыка Т.Л. Информационная безопасность: учебное пособие для студентов учреждений среднего профессионального образования 3-е изд., – М.: ИД «ФОРУМ», 2010 г.- 432 с.

Для самостоятельной работы студентов используется сеть Internet.

6.Материально-техническое обеспечение дисциплины.

Оборудование учебного кабинета:
- посадочные места по количеству обучающихся;
- автоматизированное рабочее место преподавателя;
-компьютер, ноутбук

7.Методические рекомендации по организации изучения дисциплины:

Курс трактует общие подходы к реализации информационной безопасности современного обучения. Здесь следует обратить особое внимание на то, что в переходный период к построению информационного общества информационные ресурсы становятся востребуемым продуктом,

имеющим высокую потребительскую ценность. Отсюда следует объективная необходимость развития мер защиты информации и данных.

Излагаются общие подходы к построению защищенной информационной или вычислительной системы. Основным моментом этого раздела следует считать системный подход формированию моделей угроз, общей модели информационной защиты, модели политики ИБ и структуре документов в сфере ИБ. Для каждого вида угроз необходимо выстраивать цепочку: <вид угрозы> - <оценка риска реализации> - <оценка достаточности средств защиты> - <компенсация возможного ущерба>.

Курс дисчциплины посвящен стандартам информационной безопасности. Развитие семейства стандартов следует рассматривать в контексте развития информационных технологий в целом. При этом особое внимание следует обратить на построение системы оценки рисков, которая является одной из основных составляющих общей системы безопасности. Здесь необходимо достаточно подробно рассматривать содержание современных стандартов обеспечения ИБ и информационных рисков.

Также рассматриваются современные технологии и инструменты информационной безопасности. Важным аспектом является то, что вследствие быстрого развития ИТ постоянно изменяются методы и технологии работы с информацией, появляются способы проникновения в информационные системы, а также всё новые и новые семейства вирусов. Всё это приводит к необходимости постоянного совершенствования защиты информационной инфраструктуры и необходимости построения комплексной информационной защиты ПО.

8.Перечень основной учебной литературы.

1. Белов Е.Б. и др. Проблема информационной безопасности. Учебно-методическое пособие УМО в области ИБ. – М.: ИКСИ-2004г.
2. Масленников М.Е. Практическая криптография. – СПб.: БХВ-Петербург, 2003
3. Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. - М.: Гелиос АРВ, 2004

4. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего специального образования. - М.: ФОРУМ : ИНФРА-М, 2002.
5. Практическая криптография: алгоритмя и их применение / А. В. Аргановский, Р. А. Хадди - М.: СОЛОН-Пресс, 2002
6. Федеральный Закон «Об информации, информатизации и защите информации». Собрание законодательсьва Российской Федерации 20.02.1995г.:Официальное издание. – М.: Юридическая литература; Администрация Президента Российской Федерации, 1995.
7. Фигурнов В.Э. IBM для пользователя. Краткий курс – М.:ИНФРА-М, 1998.
8. Щербаков А. Разрушающее программное воздействие. - М.:ЭДЕЛЬ, 1993.