

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Алтайский государственный институт культуры»  
Факультет информационных ресурсов и дизайна  
Кафедра информатики

«УТВЕРЖДАЮ»  
Председатель Совета факультета ИРИД  
Е. В. Валашова  
М.П.  
подпись



### **Б1.Б.16. Информационная безопасность и защита информации**

Рабочая программа учебной дисциплины,  
направление подготовки 46.03.02  
«Документоведение и архивоведение»,  
профиль – «Документоведение и  
документационное обеспечение управления»,  
квалификация выпускника – бакалавр,  
форма обучения – заочная

Общая трудоемкость часы		Семестр	Виды учебной работы, включая внеаудиторную СРС и трудоемкость (в часах)		Форма промежуточной аттестации
з.е.	часы		контактные	внеаудиторная СРС	
2	72	10	16	56	зачет (10 с)

Барнаул, 2016

Обсуждена  
на заседании кафедры  
информатики 04.02.16 г.,  
протокол № 7

Согласовано.  
на кафедре музеологии и  
документоведения  
05.02.2016, протокол № 7

Рассмотрена на заседании Методической школы факультета  
информационных ресурсов и дизайна  
12.02.2016, протокол № 3

Утверждена Советом факультета информационных ресурсов и  
дизайна  
12.02.16 г., протокол № 6

**Информационная безопасность и защита информации:** рабочая программа учебной дисциплины, направление подготовки 46.03.02 «Документоведение и архивоведение», профиль – «Документоведение и документационное обеспечение управления», квалификация выпускника – бакалавр, форма обучения – заочная / сост. К. Е. Поползин ; Алт. гос. институт культуры, каф. информатики. – Барнаул, 2016. – 25 с.

Рабочая программа учебной дисциплины «Информационная безопасность и защита информации» включает основное содержание обучения по данному курсу. В ней определены цели и задачи, структура учебного предмета, содержание разделов и тем, используемые образовательные технологии, вопросы для промежуточной аттестации, сведения об учебно-методическом, информационном и материально-техническом обеспечении дисциплины. Данная программа разработана в соответствии с требованиями ФГОС ВО.

Программа предназначена для студентов заочной формы обучения по направлению подготовки 46.03.02 «Документоведение и архивоведение».

Составитель: **К. Е. Поползин**, преподаватель

Рецензент: **О. П. Кутькина**, к.п.н, доцент

## СОДЕРЖАНИЕ

1. Пояснительная записка.....	4
2. Структура и содержание дисциплины.....	9
3. Образовательные технологии.....	17
4. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины ...	17
5. Методические указания для обучающихся по освоению дисциплины.....	19
6. Учебно-методическое и информационное обеспечение дисциплины.....	21
7. Материально-техническое обеспечение дисциплины.....	23

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

### 1.1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель освоения дисциплины: ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которыми подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации.

Задачи дисциплины: ознакомить студентов с тенденциями развития защиты информационной с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а так же с нормативными документами и методами защиты компьютерной информации.

### 1.2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» входит в раздел Б.1. Базовая часть федерального государственного образовательного стандарта высшего образования по направлению подготовки «Документоведение и архивоведение».

Для успешного освоения учебной дисциплины должны быть сформированы 4 компетенции (ОПК-6, ПК-29, ПК-12, ПК-48).

Индекс компетенции	Компетенция выпускника	Предшествующие дисциплины	Параллельные дисциплины	Последующие дисциплины
ОПК-6	способность решать стандартные задачи	Информационное право Информационные технологии	Деловое общение Стандартизация и	

	<p>профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>в документационном обеспечении управления и архивном деле Web-технологии Законодательная и нормативно-методическая база ДОУ Экспертиза ценности документа Профессиональная этика</p>	<p>унификация ДОУ и архивного дела Базы данных правовой информации</p>	
<p><b>ПК-29</b></p>	<p>владение основами информационно-аналитической деятельности и способностью применять их в профессиональной сфере</p>	<p>Математика Информационные технологии в документационном обеспечении управления и архивном деле Документные фонды предприятий Электронный документооборот Организация секретарского обслуживания Информационно-справочный</p>	<p>Организация работы с электронными документами и Автоматизированные системы документационного обеспечения управления и архивоведения</p>	<p>Организация работы с электронными документами</p>

		аппарат документационного обеспечения управления Информационное обеспечение деятельности руководителей		
<b>ПК-12</b>	способность выявлять и отбирать документы для разных типов и видов публикаций			Управление качеством документации
<b>ПК-48</b>	владение навыками оптимизации состава документов и информационных потоков, сокращения их количества	Текущее хранение дел Управленческая документация		

### **1.3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ:**

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования на 2 этапе формирования компетенций:

<b>Индекс компетенции</b>	<b>Пороговый уровень</b>	<b>Повышенный уровень</b>
<b>ОПК-6</b>	Знать: основные понятия и	Знать: основные понятия и

	<p>определения информационной безопасности; о вредоносных программах и программах защиты от компьютерных вирусов и других вредоносных программ          Уметь: выявлять и отбирать документы для разных типов и видов публикаций          Владеть: навыками оптимизации состава документов и информационных потоков; навыками оптимизации состава документов и информационных потоков в учреждении</p>	<p>определения информационной безопасности, информационно-коммуникационных технологий; риски и формы атак на информацию; угрозы, которым подвергается информация; о вредоносных программах и программах защиты от компьютерных вирусов и других вредоносных программ; о методах и средствах защиты информации          Уметь: выявлять и отбирать документы для разных типов и видов публикаций в зависимости от сложности решения задачи          Владеть: навыками оптимизации состава документов и информационных потоков, сокращения их количества; способностью разрабатывать политику компании в соответствии со стандартами безопасности; навыками оптимизации состава документов и информационных потоков в учреждении</p>
<b>ПК-29</b>	<p>Знать: источники, риски и формы атак на информацию          Уметь: классифицировать источники, риски и формы атак на информацию          Владеть: основами информационно-аналитической деятельности</p>	<p>Знать: случайные и преднамеренные источники, риски и формы атак на информацию          Уметь: классифицировать источники, риски и формы атак на информацию; выявлять и отбирать документы для разных типов и видов публикаций; решать стандартные задачи профессиональной деятельности на основе</p>

		информационной и библиографической культуры с применением информационно-коммуникационных технологий Владеть: основными методами информационно-аналитической деятельности и способностью применять их в профессиональной сфере
<b>ПК-12</b>	Знать: основы работы с документами для разных типов и видов публикаций Уметь: выявлять и отбирать документы для разных типов и видов публикаций Владеть: основными методами работы с различными источниками информации	Знать: основные методы работы с документами для разных типов и видов публикаций Уметь: выявлять и отбирать документы для разных типов и видов публикаций в зависимости от сложности решения задачи Владеть: методами работы с научно-технической литературой и источниками из Интернета
<b>ПК-48</b>	Знать: основы работы с документами для разных типов и видов публикаций Уметь: выявлять и отбирать документы для разных типов и видов публикаций Владеть: основами информационно-аналитической деятельности; навыками оптимизации состава документов и информационных потоков	Знать: основные методы работы с документами для разных типов и видов публикаций Уметь: выявлять и отбирать документы для разных типов и видов публикаций в зависимости от сложности решения задачи Владеть: основами информационно-аналитической деятельности и способностью применять их в профессиональной сфере; навыками оптимизации состава документов и информационных потоков, сокращения их количества; способностью разрабатывать политику компании в соответствии со стандартами безопасности;



		навыками оптимизации состава документов и информационных потоков в учреждении
--	--	---

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### Календарно-тематический план

Общая трудоемкость:

2 зач. ед., 72 часа, в том числе:

контактная работа – 16 часов,

внеаудиторная СРС – 56 часов;

форма промежуточной аттестации – зачет в 10 семестре.

№ п/п	Разделы и темы дисциплины	семестр	Виды учебной работы, включая внеаудиторную СРС и трудоемкость (в часах)					Формы текущего контроля успеваемости	
			лекции	семинарские	практические	лабораторные	КСР		Внеаудиторная СРС
1.	Сущность проблемы информационной безопасности в компьютерных системах	9	0,5					4	ПР-1, УО-3
2.	Основные угрозы информационной безопасности в компьютерных системах	9	0,5					8	ПР-1, ПР-4, УО-3
3.	Правовое обеспечение информационной безопасности	9	2					8	ПР-1, УО-3
4.	Информационная безопасность в среде Internet	9-10	4	2		2		6	ПР-1, УО-3
5.	Методы и средства защиты информации от несанкционированного	10	2					8	ПР-1, ПР-4, УО-3

	доступа									
6.	Криптографические методы защиты.	10				2			8	ПР-1, УО-3
7.	Защита компьютерных систем от вирусов и вредоносных программ	10	1						8	ПР-1, УО-3
8.	Политика безопасности	10	2		2				8	ПР-1,
	<b>Форма промежуточной аттестации</b>	10								зачет УО-3
	<b>Итого</b>		<b>8</b>		<b>2</b>	<b>4</b>			<b>56</b>	

## СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### **Тема 1. Сущность проблемы информационной безопасности в компьютерных системах**

Обучающийся должен иметь представление об актуальности и важности проблемы обеспечения информационной безопасности в компьютерных системах (ИБКС), предпосылках, направлениях и перспективах киберпреступности.

Обучающийся должен знать основные понятия в области информационной безопасности: информация, информационная инфраструктура, информационная система, информационный ресурс, информационная безопасность, защита информации, объект и предмет защиты, цели защиты информации.

### **Тема 2. Основные угрозы информационной безопасности в компьютерных системах**

Обучающийся должен знать **основные угрозы информационной безопасности**, характеристики информационного ресурса как объекта защиты, классификацию и характеристики угроз ИБ.

Обучающийся должен уметь различать угрозы случайные и преднамеренные, внешние и внутренние, стихийного и искусственного характера.

Обучающийся должен иметь представление о проявлениях, последствиях и основных способах реализации угроз.

### **Тема 3. Правовое обеспечение информационной безопасности**

Обучающийся должен знать: понятие правового обеспечения ИБКС, особенности информации как объекта права; основные конституционные и правовые нормы в области информационной безопасности, понятия банковской, коммерческой и служебной тайны.

Обучающийся должен иметь представление: о Государственной политике РФ в области правового обеспечения; о структуре государственных органов РФ, осуществляющих правотворчество и правоприменение в области ИБКС, о наказаниях за преступления в сфере компьютерной информации, о зарубежном законодательстве в области ИБКС.

#### **Тема 4. Информационная безопасность в среде Internet.**

Обучающийся должен иметь представление: об основных угрозах ИБ в Internet.

Обучающийся должен уметь осуществлять контроль за личной информацией.

Обучающийся должен знать: основы безопасности в социальных сетях; способы защиты электронной почты и Skype и методы защита браузера.

#### **Тема 5. Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах**

Обучающийся должен иметь представление о технических и программных средствах защиты информации в компьютерных сетях.

Обучающийся должен знать: основные методы защиты информации в компьютерных системах от несанкционированного доступа, как производится идентификация и аутентификация субъектов доступа.

Обучающийся должен уметь использовать современные системы защиты персональных ЭВМ от несанкционированного доступа к информации.

#### **Тема 6. Криптографические методы защиты.**

Обучающийся должен иметь представление: о криптологии в целом, истории возникновения, о криптографии и криптоанализе, о шифровании как методе криптографического преобразования.

Обучающийся должен знать основные методы шифрования: методы шифрования с симметричным ключом, методы замены

(подстановки) и перестановки, метод гаммирования, шифрование, использующее генераторы (датчики) псевдослучайных последовательностей, системы несимметричного шифрования: с открытым ключом для шифрования и закрытым - для дешифрования; особенности стандартизации и сертификации криптографических средств.

Обучающийся должен уметь использовать основные методы шифрования и дешифрования.

### **Тема 7. Защита компьютерных систем от вирусов и вредоносных программ**

Обучающийся должен иметь представление о компьютерных вирусах, вредоносных программах и их классификации.

Обучающийся должен знать основные методы и средства борьбы с вирусами и вредоносными программами.

Обучающийся должен уметь осуществлять профилактику заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.

### **Тема 8. Политика безопасности.**

Обучающийся должен знать, что такое политика информационной безопасности для организации, основные требования к политике безопасности, этапы ее разработки.

Обучающийся должен уметь разрабатывать политику информационной безопасности организации.

## **СЕМИНАРСКИЕ ЗАНЯТИЯ**

<b>Семестр</b>	<b>Номер темы дисциплины</b>	<b>Наименование практических занятий (краткое содержание)</b>	<b>Условия проведения семинарских занятий для обучающихся с ОВЗ и инвалидами</b>
10	4	<p><i>Тема: «Информационная безопасность в среде Internet».</i></p> <ol style="list-style-type: none"> <li>1. Безопасность электронной почты;</li> <li>2. Безопасность в Skype</li> <li>3. Защита от спама и фишинга</li> <li>4. Безопасность в социальных сетях</li> <li>5. Безопасность в интернет-банках.</li> </ol>	Дифференцированное обучение – методы индивидуального личностно ориентированного обучения с

		<p>интернет-магазинах</p> <p>6. Безопасность в играх онлайн <i>Список литературы:</i></p> <p>1. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов, обучающихся по спец-ти "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. – 5-е изд., стер. – Москва : Академия, 2011. – 336 с.</p> <p>2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. – Москва : ДМК Пресс, 2010. – 591 с. – Режим доступа: <a href="http://www.knigafund.ru">http://www.knigafund.ru</a>.</p> <p>3. Галатенко, В. А. Основы информационной безопасности [Текст]: курс лекций. Учебное пособие / В. А. Галатенко ; ред. В. Б. Бетелин. – Изд. 3-е. – Москва : Интернет-Университет информационных технологий, 2006. – 205 с.</p> <p>4. Арутюнов, В. В. Защита информации [Текст] : учеб.-методическое пособие / В. В. Арутюнов. – Москва : Либерия-Библиформ, 2008. – 56 с.</p>	<p>учетом ограниченных возможностей здоровья и личностных психолого- физиологических особенностей</p>
--	--	--	---

## ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Семе стр	Номер темы дисциплины	Наименование практических занятий (краткое содержание)	Условия проведения практических занятий для обучающихся с ОВЗ и инвалидами
10	8	Тема: « Анализ рисков информационной безопасности»	Дифференцированное обучение – методы индивидуального личностно ориентированного обучения с учетом ограниченных возможностей здоровья и личностных психолого-физиологических особенностей Письменная работа

## ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

Семе стр	Номер темы дисциплины	Наименование лабораторных занятий (краткое содержание)	Условия проведения лабораторных занятий для обучающихся с ОВЗ и инвалидами
10	4	Тема: «Настройка браузера и электронной почты для обеспечения безопасности в Интернет»	Дифференцированное обучение – методы индивидуального личностно ориентированного обучения с учетом ограниченных возможностей здоровья и личностных психолого-физиологических особенностей Задания и метод. указания к ним размещены в Moodle
10	6	Тема: «Простые шифры. Разработка и анализ простых криптографических алгоритмов на основе методов перестановок и подстановок»	Дифференцированное обучение – методы индивидуального личностно ориентированного обучения с учетом ограниченных возможностей здоровья и личностных психолого-физиологических особенностей Задания и метод.

			указаний к ним размещены в Moodle
--	--	--	-----------------------------------

### **КОНТАКТНАЯ (КОНТРОЛИРУЕМАЯ) САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ**

<b>Семес тр</b>	<b>Номер темы дисципли ны</b>	<b>Тема для изучен ия</b>	<b>Форма проведен ия занятий</b>	<b>Форма внеаудиторн ой СРС для обучающихс я с ОВЗ и инвалидами</b>	<b>Количес тво часов</b>
Не предусмотрена					

### **ВНЕАУДИТОРНАЯ СРС (КОНТАКТНЫЕ ЧАСЫ)**

<b>Семестр</b>	<b>Номер темы дисци плины</b>	<b>Тема для изучения</b>	<b>Форма внеаудит орной СРС</b>	<b>Форма внеаудит орной СРС для обучающ ихся с ОВЗ и инвалида ми</b>	<b>Количес тво часов</b>
7	1.	Сущность проблемы информационной безопасности в компьютерных системах	Подготовка докладов	Устно, письменное	4
7	2.	Основные угрозы информационной безопасности	Подготовка докладов	Устно, письменное	8



		компьютерных системах			
7	3.	Правовое обеспечение информационной безопасности	Индивидуальные задания	Устно, письменное	8
7	4.	Информационная безопасность в среде Internet	Индивидуальные задания	Устно, письменное	6
7	5.	Методы и средства защиты информации от несанкционированного доступа	Индивидуальные задания	Устно, письменное	8
7	6.	Криптографические методы защиты.	Индивидуальные задания	Устно, письменное	8
7	7.	Защита компьютерных систем от вирусов и вредоносных программ	Индивидуальные задания	Устно, письменное	8
7	8.	Политика безопасности	Индивидуальные задания	Устно, письменное	8

**Учебно-методическое обеспечение  
для самостоятельной работы обучающихся**

**Информационная безопасность и защита информации:** методические указания к самостоятельной работе студента, направление подготовки 46.03.02 «Документоведение и архивоведение», профиль подготовки «Документоведение и документационное обеспечение управления», квалификация выпускника – бакалавр, форма обучения – очная, заочная / сост. К. Е. Поползин ; АГИК, каф. информатики. – Барнаул, 2016.

### **3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ** (в интерактивной форме 2 часа)

Номер темы дисциплины	Темы для изучения	Наименование разработанных, используемых новых педагогических технологий и инновационных методов обучения*	Наименование адаптированных методов обучения для обучающихся с ОВЗ и инвалидов
4	Информационная безопасность в среде Internet	Лекция-визуализация	Индивидуальные методы обучения

### **4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

Информационная безопасность и защита информации: фонд оценочных средств, направление подготовки 46.03.02 «Документоведение и архивоведение», профиль подготовки «Документоведение и документационное обеспечение управления», квалификация выпускника – бакалавр, форма

обучения – очная, заочная / сост. К.Е. Поползин ; АГИК, каф. информатики. – Барнаул, 2016.

### **Примерные вопросы для самоподготовки к зачету**

1. Важность проблемы информационной безопасности (ИБ) компьютерных систем.
2. Актуальность проблемы ИБ.
3. Сущность проблемы ИБ.
4. Понятие информационной безопасности (ИБ).
5. Задачи защиты информации.
6. Угрозы ИБ, классификация угроз.
7. Основные угрозы ИБ естественного характера.
8. Случайные угрозы ИБ.
9. Преднамеренные угрозы ИБ.
10. Угрозы для каналов и линий связи вычислительных сетей.
11. Виды обеспечения ИБ.
12. Характеристика правового обеспечения ИБ.
13. Проблемы правового обеспечения ИБ.
14. Задачи государства в области ИБ.
15. Основные законодательные акты в области ИБ.
16. Понятие банковской тайны, коммерческой тайны и служебной тайны.
17. Ответственность за компьютерные преступления.
18. Понятие организационного обеспечения ИБ.
19. Задачи организационного обеспечения ИБ.
20. Сущность идентификации и аутентификации.
21. Сущность произвольного доступа в КС.
22. МетодыЗИ от случайных угроз.
23. МетодыЗИ в КС от традиционного шпионажа и диверсий.
24. Методы защиты от несанкционированного доступа.
25. Криптографические методыЗИ.
26. Понятие электронной подписи.

27. Методы защиты компьютерных сетей от не санкционированного доступа к информации.
28. Понятие компьютерного вируса.
29. Понятие и классификация вредоносных программ.
30. Классификация компьютерных вирусов.
31. Классификация средств защиты от компьютерных вирусов.
32. Обязанности пользователей по обеспечению ИБ.

### Критерии оценки

Показатели оценки	Полнота	Терминология	Структура изложения
зачтено	<p>Демонстрирует владение компетенциями.</p> <p>Вопрос раскрыт полно, осмысленно, глубоко: с опорой на концепции ведущих авторов, нормативные документы.</p> <p>Приведены примеры.</p> <p>Допущены незначительные фактические неточности</p>	Хорошее владение понятийно-терминологическим аппаратом.	Ответ четко выстроен, изложение последовательное, уверенное, осознанное.
не зачтено	<p>Не владеет компетенциями.</p> <p>Фрагментарное неглубокое раскрытие вопроса.</p>	Не полное владение основными понятиями.	Ответ неуверенный, слабо выстроен.

	Допущены принципиальные неточности.		
--	-------------------------------------	--	--

## **5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

Рабочая программа дисциплины включает темы, которые выстроены в четко определенной логике, предусматривающей структурирование учебного материала от общих теоретико-методологических вопросов к частным. В каждой теме определены все необходимые для обязательного изучения вопросы. По всем темам сформулированы контрольные вопросы для самопроверки степени усвоения знаний. Студентам в ходе самостоятельной работы над темами рекомендуется ответить на все предложенные вопросы, чтобы понять какие из них вызывают затруднения. В ходе изучения дисциплины проводится текущий контроль знаний в форме тестовых испытаний, также выполняющие для студента функцию самоконтроля.

Ввиду того, что многие теоретические понятия не имеют однозначной трактовки в учебной и научной литературе, учебно-методический комплекс дисциплины включает учебный терминологический словарь, которым может воспользоваться обучающийся для овладения категориальным аппаратом дисциплины.

Для подготовки к семинарским занятиям в программе предложен минимум основных источников, которые дадут возможность обучающемуся изучить проблему, вынесенную для обсуждения на семинарском занятии и принять участие в учебной дискуссии. Для подготовки докладов следует воспользоваться рекомендованным списком дополнительной литературы. Обучающийся в процессе самостоятельной работы может также пользоваться ресурсами Интернет, которые являются одним из альтернативных источников быстрого поиска требуемой

информации. Их использование возможно для получения основных и дополнительных сведений по изучаемым материалам.

В процессе изучения дисциплины используются традиционные и инновационные (интерактивные) образовательные технологии: лекции (лекция-визуализация); семинарские занятия, практические занятия.

## **6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **а) основная литература:**

Аверченков, В. И. Организационная защита информации [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Москва : Флинта, 2011. – 184 с. – Режим доступа : <http://www.knigafund.ru>

Аверченков, В. И. Служба защиты информации: организация и управление [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Москва : Флинта, 2011. – 186 с. – Режим доступа : <http://www.knigafund.ru>

Арутюнов, В. В. Защита информации [Текст] : учеб.-методическое пособие / В. В. Арутюнов. – Москва : Либерей-Бибинформ, 2008. – 56 с.

Клейменов, С. А. Информационная безопасность и защита информации [Текст] : учебное пособие. – Москва : Академия, 2011. – 336 с.

Креопалов, В. В. Технические средства и методы защиты информации [Электронный ресурс] : учебно-практическое пособие / В. В. Креопалов. – Москва : Евразийский открытый ин-т, 2011. – 278 с. – Режим доступа : <http://www.http://нэб.рф>

Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников. – [Б. м.] : Академия, 2011. – 336 с.

### **б) дополнительная литература:**

Алешин, Л. И. Безопасность в библиотеке [Текст] : учеб.-метод. пособие / Л. И. Алешин. – М. : Либерей-Бибинформ, 2005. – 247 с.

Галатенко, В. А. Основы информационной безопасности [Текст] : курс лекций : учебное пособие / В. А. Галатенко; ред. В. Б. Бетелин. – Изд. 3-е. – Москва : Интернет-университет информационных технологий, 2006. – 205 с.

Галатенко, В. А. Стандарты информационной безопасности [Текст]: курс лекций : учебное пособие / В. А. Галатенко; В. Б. Бетелин. – Изд. 2-е. – Москва : Интернет-университет информационных технологий, 2006. – 263 с.

Городов, О. А. Информационное право [Текст]: учебник / О. А. Городов. – Москва : Проспект; ТК Велби, 2008. – 242 с.

Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – Москва : Академический Проект, 2006. – 331 с.

Сергеева Ю. С. Защита информации [Электронный ресурс] : конспект лекций / Ю. С. Сергеева. – Москва : А-Приор, 2011. – 128 с. – Режим доступа : [http://www. http://нэб.рф](http://www.http://нэб.рф)

Смирнов, А. А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс] : монография / А. А. Смирнов. – Москва : Юнити-Дана; Закон и право, 2012. – 159 с. – Режим доступа : <http://www.knigafund.ru>

#### **в) информационные технологии: программное обеспечение и Интернет-ресурсы:**

ОС Windows

Пакет MS Office

Интернет-браузер

Информационно-поисковые системы сети Интернет

Электронные каталоги и ресурсы web-сайтов следующих организаций:

– российской образование: федеральный портал ([www.edu.ru](http://www.edu.ru));

– российская государственная библиотека ([www.rsl.ru](http://www.rsl.ru));

– российская библиотечная ассоциация ([www.rba.ru](http://www.rba.ru));

– российская национальная библиотека ([www.nlr.ru](http://www.nlr.ru));

– электронная библиотека Алт.гос. институт культуры ([www.altgaki.org/2011-02-10-09-23-53](http://www.altgaki.org/2011-02-10-09-23-53)).

– ЭБС «Книгафонд» [http://www.knigafund.ru/](http://www.knigafund.ru)

#### **г) аудиокниги, фонограммы, пособия для незрячих**

Каждый студент обеспечен доступом к электронно-библиотечной системе АГИК, содержащей издания по дисциплине<sup>1</sup>, к ЭБС Книгафонд 2а также к Национальной электронной библиотеке.<sup>3</sup>

---

<sup>1</sup> Режим доступа <http://agaki.ru/biblioteka-news/informacziionnye-resursy/elektronnaya-biblioteka>



Для обучающихся с нарушением зрения учебно-методическое обеспечение дисциплины осуществляется на основании Договора о сотрудничестве АГИК с Алтайской краевой специальной библиотекой для незрячих и слабовидящих № 27 от 20.11.2015 г.

Библиотечный фонд укомплектован печатными изданиями основной учебной литературы по дисциплине. Фонд дополнительной литературы, помимо учебной, включает официальные, справочные и специализированные периодические издания.

Ресурсы Алтайской краевой специальной библиотеки для незрячих и слабовидящих (<http://bibl22.ru/>)

## **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для обеспечения дисциплины используются: лаборатория и кабинет кафедры информатики и музеологии и документоведения, компьютерный класс и аудитория для самостоятельной работы студентов факультета информационных ресурсов и дизайна, специализированные аудитории с презентационным оборудованием и наглядными материалами, библиотеки АГИК.

Для обеспечения дисциплины необходимы:

- Лекционная аудитория с мультимедийным оборудованием (экран, проектор, ноутбук).
- Компьютерный класс.
- Лицензионное программное обеспечение: ОС Windows, пакет MS Office, Интернет-браузер.
- Доступ в Интернет.
- Доступ к ЭБС.

---

<sup>2</sup> ООО «Центр цифровой дистрибуции», контракт № 0317100013415000009-01 от 10.03.2015 года.

<sup>3</sup> ФГБОУ «Российская национальная библиотека», Договор № 191/НЭБ/0433 от 15.07.2015 года

Режим доступа: <http://нэб.рф/>;

Учебное издание  
Информационная безопасность  
и защита информации

Рабочая программа учебной дисциплины  
Составитель: К. Е. Поползин

Издано на кафедре информатики  
Алтайский государственный институт культуры  
656055 г. Барнаул, ул. Юрина, 277