МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИСТОРИКО-АРХИВНЫЙ ИНСТИТУТ

Факультет архивоведения и документоведения
Кафедра архивоведения

Информационная безопасность в архивной сфере

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

46.03.02 «Документоведение и архивоведение»
Код и наименование направления подготовки/специальности

Электронные архивы и документы
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очно-заочная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Архивоведение
Рабочая программа дисциплины

к.и.н., доцент, зав. кафедрой архивоведения Е.М. Бурова

……

УТВЕРЖДЕНО
Протокол заседания кафедры
№ 3 от 01.04.2022 г.

Оглавление

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины - изучение теоретических и прикладных вопросов информационной безопасности и защиты информации в сфере документооборота и архивного дела в Российской Федерации.

Задачи дисциплины:

изучить исторические этапы развития информационной безопасности и защиты информации;

освоить терминологию и понятийный аппарат в области информационной безопасности и защиты информации;

изучить нормативно-правовую базу, регулирующую сферу информационной безопасности и защиты информации;

изучить основные средства и методы обеспечения информационной безопасности;

научить определять угрозы, уязвимости и риски информационной безопасности;

обучить навыкам защиты информации;

научить применять полученные знания и навыки по информационной безопасности и защите информации в сфере документооборота и архивного дела.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК- 4 - Способность создавать и вести системы документационного обеспечения управления архивов на базе новейших технологий	ПК-4.2 - Способен анализировать ситуацию на рынке информационных продуктов и услуг, давать экспертную оценку современным системам электронного документооборота и ведения электронного архива	Знать: историю, современное состояние, проблемы и тенденции развития систем информационной безопасности и защиты информации; нормативно-правовую базу обеспечения информационной безопасности и защиты информации; систему органов власти, определяющих и реализующих государственную политику в области информационной безопасности и защиты информации; систему документационного обеспечения информационной безопасности и защиты информации; место и роль информационной безопасности и защиты информации в области документооборота и

		архивного дела; методы и средства обеспечения информационной безопасности и защиты информации. *Уметь:* Анализировать проблемы информационной безопасности и защиты информации в системах документооборота и архивном деле; применять отечественные и зарубежные стандарты в области информационной безопасности и защиты информации; определять угрозы, уязвимости и риски информационной безопасности; *Владеть:* Терминологией и понятийным аппаратом в области информационной безопасности и защиты информации; навыками использования методов и средств обеспечения информационной безопасности и защиты информации; навыками разработки документационного обеспечения информационной безопасности и защиты информации.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина *(модуль)* «Информационная безопасность и защита информации» относится к формируемой участниками образовательных отношений блока дисциплин учебного плана подготовки бакалавров 46.03.02 «Документоведение и архивоведение».

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин и прохождения практик:

- Безопасность жизнедеятельности;
- Информатика;
- Информационные технологии;
-Основы информационного права.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик:

- Стандартизация документационного обеспечения управления и архивного дела;
- Основы архивного права;

- Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 2 з.е., 72 академических часа (ов).

Структура дисциплины для очно-заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
9	Лекции	**12**
9	Семинары/лабораторные работы	**16**
	Всего:	**28**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 44 академических часа(ов).

3. Содержание дисциплины

Введение в дисциплину

Феномен защиты информации. История ИБ и ЗИ. Специфика ИБ и ЗИ в цифровую эпоху. Место ИБ в комплексной безопасности личности, общества, государства, глобального мира. Информационное противоборство и информационные войны. Киберпреступность

Современное состояние ИБ и ЗИ. Тенденции развития. Специфика предметной области. Культура информационной безопасности. Место курса среди других изучаемых дисциплин. План и организация курса.

Раздел 1. Терминологический и понятийный аппарат информационной безопасности и защиты информации

Проблемы терминологии: многозначность, неоднозначность, трудности перевода. Понятие «информационная безопасность» в доктринальных, концептуальных, законодательных документах Российской Федерации. Объекты ИБ, угрозы и уязвимости объектов ИБ. Стандартизация терминологии. Понятия «информационная безопасность» и «защита информации» в международных и российских стандартах. Свойства ИБ: конфиденциальность, целостность, доступность и др.

Раздел 2. Теоретические и прикладные основы информационной безопасности и защиты информации

Методологические основы теории ИБ. Математический аппарат ИБ и ЗИ. Физические основы ЗИ. Программные системы обеспечения ИБ и ЗИ.

Раздел 3. Методы и средства обеспечения информационной безопасности и защиты информации

Методическое обеспечение ИБ и ЗИ. Правовое обеспечение ИБ и ЗИ. Методы и средства

обеспечение безопасности информации, процессов обработки информации, программно-технических систем, каналов связи. Технические средства обеспечения ИБ и ЗИ. Программные средства обеспечения ИБ и ЗИ. Организационные методы обеспечения ИБ и ЗИ. Современные средства ЗИ. Идентификация угроз ИБ, ранжирование угроз ИБ. Управление рисками ИБ, методы оценки рисков ИБ. Методы и средства обеспечения ИБ и ЗИ отдельных направлений: работа в Интернет, мобильные устройства, персональные данные, национальная безопасность. Защита объекта информатизации.

Раздел 4. Информационная безопасность Российской Федерации
ИБ личности, общества, государства. Доктрина информационной безопасности. Система обеспечения ИБ. Законотворчество в области ИБ и ЗИ: Комитет ГД РФ по безопасности и противодействию коррупции. Нормативная правовая база ИБ и ЗИ. ФЗ «Об информации, информационных технологиях и о защите информации», «О защите персональных данных» и др. Органы, определяющие и реализующие политику в области ИБ и ЗИ: Совет безопасности, ФСТЭК, ФСБ, Управление «К» МВД и др. Гражданские инициативы в области ИБ и ЗИ. Информационная безопасность отдельных сфер деятельности (на примере банковской сферы и сферы культуры). Информационная безопасность в РГГУ.

Раздел 5. Документационное обеспечение информационной безопасности и защиты информации
Система документов по ИБ и ЗИ. Место данных документов в системе ДОУ. Международные и национальные стандарты ИБ и ЗИ. Стандарты серии 2700х. Виды типовых документов ИБ и ЗИ. Анализ документов по обеспечению ИБ: концепция ИБ, оценка информационных активов, модели угроз и рисков информационной безопасности, оценка уязвимостей, меры обеспечения ИБ, оценка эффективности системы ИБ, политики ИБ.

Раздел 6. Комплексная безопасность информационных активов
Традиционные и цифровые информационные активы. Виды информационных активов. Взаимосвязь оценок традиционных и цифровых активов. Методика оценки информационных активов. Угрозы информационным активам. Управление рисками безопасности информационным активам. Комплексная безопасность электронного документооборота. Безопасность государственных информационных ресурсов. Комплексная безопасность Архивного фонда Российской Федерации.

4. Образовательные технологии

№ п/п	*Наименование раздела*	*Виды учебной работы*	*Информационные и образовательные технологии*
1.	Введение	Лекция 1. Самостоятельная работа	Вводная лекция с использованием Интернет-ресурсов Подготовка доклада
2.	Раздел 1. Терминологический, понятийный аппарат ИБ и ЗИ	Лекция 2. Лабораторная работа 1. Самостоятельная работа	Проблемная лекция лекция с использованием Интернет-ресурсов Развернутая беседа с обсуждением доклада

3.	Раздел 2. Теоретические и прикладные основы ИБ и ЗИ	Лекция 3. Лабораторная работа 2. Семинар 2. Самостоятельная работа	Проблемная лекция с использованием Интернет-ресурсов Работа с Интернет-ресурсами Развернутая беседа с обсуждением доклада Дискуссия Реферат
4.	Раздел 3. Методы и средства обеспечения ИБ и ЗИ	Лекция 4. Лабораторная работа 3. Самостоятельная работа	Проблемная лекция Развернутая беседа с обсуждением контрольной работы Контрольная работа
5.	Раздел 4.	Лекции 5	Проблемные лекции
	Информационная безопасность Российской Федерации	Лекция 6 Лабораторная работа 4. Самостоятельная работа	Лекции с разбором конкретной ситуации Развернутая беседа Дискуссия Подготовка к опросу
6.	Раздел 5. Документационное обеспечение ИБ и ЗИ	Лекция 6. Лабораторная работа 5. Самостоятельная работа	Проблемная лекция Работа с Интернет-ресурсами, подготовка к контрольной работе Дискуссия Консультирование и проверка домашних заданий посредством электронной почты Контрольная работа
7.	Раздел 6. Комплексная безопасность информационных активов	Лекция 7. Лабораторная работа 6. Самостоятельная работа	Лекция с использованием Интернет-ресурсов и разбором конкретных ситуаций Работа с Интернет-ресурсами. Дискуссия Подготовка к опросу

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- участие в дискуссии на семинаре* *- тест или реферат*	 *5 баллов* *30 баллов*	 *30 баллов* *30 баллов*
Промежуточная аттестация *Зачёт с оценкой*		*40 баллов*
Итого за семестр		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерная тематика рефератов (темы для эссе, докладов)

1. Сравнительный анализ обеспечения ИБ бумажных, технотронных и цифровых документов.
2. Значение и роль ИБ в обеспечении национальной безопасности Российской Федерации. 3. Организация системы ИБ и ЗИ в Российской Федерации.
4. Роль ФСТЭК в реализации государственной политики в области ИБ и ЗИ. 5. Нормативно-правовое обеспечение ИБ и ЗИ.
6. Система документационного обеспечения ИБ и ЗИ. 7. Стандарты, регулирующие ИБ.
8. Стандарты серии 2700х.
9. ИБ вуза (на примере ИАИ).
10. Анализ информационных активов РГГУ.
11. Информационные риски использования гаджетов.
12. Анализ рисков электронного документооборота.
13. Проблемы обеспечения ИБ Архивного фонда Российской Федерации.

Контрольные вопросы и задания для промежуточной аттестации по итогам освоения дисциплины:

1. Значение и роль ИБ в комплексной безопасности личности, общества, государства.
2. Основные этапы развития ИБ и ЗИ.
3. Понятие «информационная безопасность», понятие «защита информации»
4. Основные термины и понятия ИБ и ЗИ.
5. Объекты ИБ.
6. Угрозы, уязвимости, риски объектам ИБ.
7. Нормативно-правовая база обеспечения ИБ и ЗИ в Российской Федерации.
8. Доктрина информационной безопасности Российской Федерации.
9. Основные виды документов по обеспечению ИБ и ЗИ.
10. Меры и средства обеспечения ИБ и ЗИ.
11. Стандарты ИБ и ЗИ.
12. Стандарты серии 2700х.
13. Современные методы и средства ИБ и ЗИ.
14. Безопасность информационных активов.
15. Информационная безопасность Архивного фонда Российской Федерации.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

а) основные источники

Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года // Российская газета. 2009, 21 января

Указ Президента Российской Федерации от 12 мая 2009 г. N 537// Российская газета. 2009, 19 мая.

Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212 // Российская газета. 2008, 16 февраля

ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М., 2007.

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2007.

ГОСТ Р ИСО/МЭК 27003-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. М., 2007.

ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011.

ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013.

б) дополнительные источники

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 // Российская газета. 2013, 22 мая

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N 17 г. Москва // Российская газета. 2013, 22 мая.

[Методический документ]. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена приказом ФСТЭ России 14 февраля 2008 г. http://fstec.ru

[Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014). URL: http://fstec.ru

в) основная литература

Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2016. -322 с. (Высшее образование) ISBN 978-5-369-01450-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/495249

2. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - Москва: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; - (Высшее образование: Бакалавриат). ISBN 978-5-00091-007-8. - Текст: электронный. -URL: https://znanium.com/catalog/product/491597
3. Некраха А.В. Шевцова Г.А. Организация конфиденциального делопроизводства и защита информации. М., 2007.
4. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефиров С.Л., Голованов В.Б. - М.: ЦИПСиР, 2011. - 373 с. ISBN 978-5-9614-1364-9 - Режим доступа:

http://znanium.com/catalog/product/556539

Периодические издания

1. Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». М., [с 2015].
2. Вестник РГГУ. Серия «Информатика. Защита информации. Математика». М.., [2009-2014].

г) дополнительная литература

1. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - Москва: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с. + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). ISBN 978-5-369-01379-3. - Текст: электронный. - URL: https://znanium.com

2. Бирюков А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. -2-е изд., перераб. и доп. - Москва: ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1028060
3. Дубинин Е. А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - Москва: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; + 11 с. - (Научная мысль). ISBN 978-5-369-01371-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/471787
4. Кузнецов И. Н. Бизнес-безопасность / Кузнецов И.Н., - 4-е изд. - Москва: Дашков и К, 2016. - 416 с.: ISBN 978-5-394-02654-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/430343
5. Хорев П. Б. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - Москва: Форум, НИЦ ИНФРА-М, 2015. - 352 с. (Высшее образование) ISBN 978-5-00091-004-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/489084

Периодические и сериальные издания

1. Безопасность информационных технологий: научный журнал. – М. 2.
Джет Инфо: бюллетень. – М.
3. Защита информации: научный журнал. – М.
4. Защита информации. Конфидент: научный журнал. – М. 5.
Информационная безопасность: научный журнал. – СПб. 6.
Информационные войны: научный журнал. – М.
7. Открытые Системы. СУБД: научный журнал. – М.

Интернет

1. Совет безопасности Российской Федерации [офиц. сайт]. http://www.scrf.gov.ru/ 2.
Федеральная служба по техническому и экспортному контролю [офиц. сайт].
http://fstec.ru
3. Управление «К» МВД России [офиц. сайт].
https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii
4. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт].
http://www.rsuh.ru/iint
5. Методические пособия, рекомендации, перечни [офиц. сайт Федерального архивного агентства]. http://archives.ru/documents/methodics.shtml.
6. Информационная безопасность организаций банковской системы Российской Федерации [офиц. сайт Центрального банка Российской Федерации].
http://www.cbr.ru/credit/gubzi_docs

7. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт]. http://www.rsuh.ru/iintb

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases
Профессиональные полнотекстовые базы данных:

1. Национальная электронная библиотека (НЭБ) www.rusneb.ru
2. ELibrary.ru Научная электронная библиотека www.elibrary.ru
3. Электронная библиотека Grebennikon.ru www.grebennikon.ru
4. Cambridge University Press
5. ProQuest Dissertation & Theses Global
6. SAGE Journals
7. Taylor and Francis
8. JSTOR

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером и проектором для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Adobe Master Collection
5. AutoCAD
6. Archicad
7. SPSS Statisctics
8. ОС «Альт Образование»
9. Visual Studio
10. Adobe Creative Cloud

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы семинарских/ практических/ лабораторных занятий

Раздел 1. Терминологический и понятийный аппарат ИБ и ЗИ (2 час.) *Цель занятия* – изучение терминологического и понятийного аппарата ИБ и ЗИ. *Форма проведения* – лабораторная работа с Интернет-ресурсами.

Вопросы для обсуждения:

Значение и роль ИБ в комплексной безопасности личности, общества, государства.

Основные этапы развития ИБ и ЗИ.

Контрольные вопросы:

Понятие «информационная безопасность», понятие «защита информации»

Основные термины и понятия ИБ и ЗИ.

Список источников и литературы:

источники (основные, дополнительные):

Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года // Российская газета. 2009, 21 января

Указ Президента Российской Федерации от 12 мая 2009 г. N 537// Российская газета. 2009, 19 мая.

Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212 // Российская газета. 2008, 16 февраля

ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М., 2007.

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2007.

дополнительные источники

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 // Российская газета. 2013, 22 мая

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N 17 г. Москва // Российская газета. 2013, 22 мая.

литература

Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2016. -322 с. (Высшее образование) ISBN 978-5-369-01450-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/495249

2. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - Москва: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил. - (Высшее образование: Бакалавриат). ISBN 978-5-00091-007-8. - Текст: электронный. -URL: https://znanium.com/catalog/product/491597
3. Некраха А.В. Шевцова Г.А. Организация конфиденциального делопроизводства и защита информации. М., 2007.

Раздел 2. Теоретические и прикладные основы ИБ и ЗИ (2 час.)

Цель занятия – изучение теоретических основ и прикладных вопросов ИБ и ЗИ.

Форма проведения – лабораторная работа с Интернет-ресурсами.

Вопросы для обсуждения:

Сравнительный анализ обеспечения ИБ бумажных, технотронных и цифровых документов.

Контрольные вопросы:

Методологические основы теории ИБ. Математический аппарат ИБ и ЗИ. Физические основы ЗИ. Программные системы обеспечения ИБ и ЗИ.

Список источников и литературы:

источники (основные, дополнительные):

ГОСТ Р ИСО/МЭК 27003-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. М., 2007.

ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011.

ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013

литература (основная, дополнительная)

1. Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». М., [с 2015].
2. Вестник РГГУ. Серия «Информатика. Защита информации. Математика». М.., [2009-2014].
3. Бирюков А. А. Информационная безопасность: защита и нападение. М., 2013. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. М., 2015.
4. Галатенко В.А. Основы информационной безопасности: учеб. пособие: для студентов вузов, обучающихся по специальности «Прикладная информатика» / [под ред. В. Б. Бетелина]. М., 2008.
5. Сохранение электронной информации в информационном обществе. Сборник материалов Международной конференции (Москва, 3 – 5 октября 2011 г.). М., 2011.
6. Тихонов В.И. Информационные технологии и электронные документы в контексте архивного дела (статьи разных лет). — М., 2009.
7. Хорев П. Программно-аппаратная защита информации. Учебное пособие. М., 2015.
8. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М., 2016.

Раздел 3. Методы и средства обеспечения ИБ и ЗИ (2 **час.)**

Цель занятия – изучение основных методов и средств обеспечения ИБ и ЗИ.

Форма проведения – лабораторная работа с Интернет-ресурсами.

Вопросы для обсуждения: Объекты ИБ. Угрозы, уязвимости, риски объектам ИБ. Современные методы и средства ИБ и ЗИ.

Контрольные вопросы:

Методическое обеспечение ИБ и ЗИ. Правовое обеспечение ИБ и ЗИ. Методы и средства обеспечение безопасности информации, процессов обработки информации, программно-технических систем, каналов связи. Технические средства обеспечения ИБ и ЗИ. Программные средства обеспечения ИБ и ЗИ. Организационные методы обеспечения ИБ и ЗИ.

Список источников и литературы:

источники (основные, дополнительные):

ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М., 2007

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2007.

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011.

ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013.

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 // Российская газета. 2013, 22 мая

литература (основная, дополнительная)

1. Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». М., [с 2015].
2. Вестник РГГУ. Серия «Информатика. Защита информации. Математика». М.., [2009-2014].
3. Бирюков А. А. Информационная безопасность: защита и нападение. М., 2013. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. М., 2015.
4. Галатенко В.А. Основы информационной безопасности: учеб. пособие : для студентов вузов, обучающихся по специальности «Прикладная информатика» / [под ред. В. Б. Бетелина]. М., 2008.
5. Сохранение электронной информации в информационном обществе. Сборник материалов Международной конференции (Москва, 3 – 5 октября 2011 г.). М., 2011.
6. Тихонов В.И. Информационные технологии и электронные документы в контексте архивного дела (статьи разных лет). — М., 2009.
7. Хорев П. Программно-аппаратная защита информации. Учебное пособие. М., 2015. 8.

Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М., 2012.

Раздел 4. Информационная безопасность Российской Федерации (2 час.)

Цель занятия – изучение правовых, организационных и иных вопросов обеспечения информационной безопасности Российской Федерации.

Форма проведения – лабораторная работа с Интернет-ресурсами.

Вопросы для обсуждения: Значение и роль ИБ в обеспечении национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.

Контрольные вопросы:

Система обеспечения ИБ. Законотворчество в области ИБ и ЗИ: Комитет ГД РФ по безопасности и противодействию коррупции. Нормативная правовая база ИБ и ЗИ. ФЗ «Об информации, информационных технологиях и о защите информации», «О защите персональных данных» и др. Органы, определяющие и реализующие политику в области ИБ и ЗИ.

Список источников и литературы:

источники (основные, дополнительные):

1. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное

пособие / Е.К.Баранова, А.В.Бабаш - Москва: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с. + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). ISBN 978-5-369-01379-3. - Текст: электронный. - URL: https://znanium.com

2. Бирюков А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. -2-е изд., перераб. и доп. - Москва: ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1028060
3. Дубинин Е. А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - Москва: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; + 11 с. - (Научная мысль). ISBN 978-5-369-01371-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/471787
4. Кузнецов И. Н. Бизнес-безопасность / Кузнецов И.Н., - 4-е изд. - Москва: Дашков и К, 2016. - 416 с.: ISBN 978-5-394-02654-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/430343
5. Хорев П. Б. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - Москва: Форум, НИЦ ИНФРА-М, 2015. - 352 с. (Высшее образование) ISBN 978-5-00091-004-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/489084

Раздел 5. Документационное обеспечение ИБ и ЗИ (2 час.)

Цель занятия – изучение комплекса документов по обеспечению ИБ и ЗИ. Изучение документов, возникающих при обеспечении ИБ и ЗИ.

Форма проведения – лабораторная работа с Интернет-ресурсами.

Вопросы для обсуждения: Основные виды документов по обеспечению ИБ и ЗИ. Место данных документов в системе ДОУ. Международные и национальные стандарты ИБ и ЗИ.

Контрольные вопросы:

Нормативно-правовое обеспечение ИБ и ЗИ. Система документационного обеспечения ИБ и ЗИ. Стандарты, регулирующие ИБ. Стандарты серии 2700х.

Список источников и литературы:

источники (основные, дополнительные):

Федеральный закон от 27 июля 2006 г. N 149-ФЗ // Российская газета. 2006, 29 июля

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2007.

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 // Российская газета. 2013, 22 мая

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N 17 г. Москва // Российская газета. 2013, 22 мая

Литература

1. Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». М., [с 2015].
2. Вестник РГГУ. Серия «Информатика. Защита информации. Математика». М.., [2009-2014].

3. Бирюков А. А. Информационная безопасность: защита и нападение. М., 2013. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. М., 2015.
4. Галатенко В.А. Основы информационной безопасности: учеб. пособие : для студентов вузов, обучающихся по специальности «Прикладная информатика» / [под ред. В. Б. Бетелина]. М., 2008.
5. Сохранение электронной информации в информационном обществе. Сборник материалов Международной конференции (Москва, 3 – 5 октября 2011 г.). М., 2011.
6. Тихонов В.И. Информационные технологии и электронные документы в контексте архивного дела (статьи разных лет). — М., 2009.
7. Хорев П. Программно-аппаратная защита информации. Учебное пособие. М.,2015.

Раздел 6. Комплексная безопасность информационных активов (2 час.)

Цель занятия – изучение комплексной безопасности информационных активов. Изучение информационной безопасности Архивного фонда Российской Федерации.

Форма проведения – лабораторная работа с Интернет-ресурсами.

Вопросы для обсуждения:

Анализ информационных активов РГГУ. Проблемы обеспечения ИБ Архивного фонда Российской Федерации.

Контрольные вопросы:

Безопасность информационных активов. Оценка информационных активов. Оценка рисков информационным активам.

Список источников и литературы:

источники (основные, дополнительные):

Указ Президента Российской Федерации от 09 сентября 2000 г. N 1895.Российская газета 19 мая 2009 г.

ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013

Об утверждении Требованийо защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N 17 г. Москва // Российская газета. 2013, 22 мая

литература (основная, дополнительная)

1. Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». М., [с 2015].
2. Вестник РГГУ. Серия «Информатика. Защита информации. Математика». М.., [2009-2014].
3. Бирюков А. А. Информационная безопасность: защита и нападение. М., 2013. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. М., 2015.
4. Галатенко В.А. Основы информационной безопасности: учеб. пособие: для студентов вузов, обучающихся по специальности «Прикладная информатика» / [под ред. В. Б. Бетелина]. М., 2008.
5. Сохранение электронной информации в информационном обществе. Сборник материалов Международной конференции (Москва, 3 – 5 октября 2011 г.). М., 2011.
6. Тихонов В.И. Информационные технологии и электронные документы в контексте архивного дела (статьи разных лет). — М., 2009

9.2 Методические рекомендации по подготовке письменных работ

Контрольная работа должна представлять собой самостоятельный ответ на вопросы. Реферат как краткий обзор публикаций по заданной теме, с элементами сопоставительного анализа, передает авторскую позицию изложение собственного видения проблемы. Необходимо грамотно изложить материал в соответствии с той или иной логикой (хронологической, тематической и др.). Реферат должен содержать итоги проведенной исследовательской работы. Начинается реферат с титульного листа, за которым следует оглавление - план, в котором каждому разделу должен соответствовать номер страницы. Основная часть может быть представлена как цельным текстом, так и разделена на главы. Заключение должно содержать краткие и четкие выводы. Завершается реферат списком источников и литературы. В работе должно быть использовано не менее 5 разных источников. Оформление списка источников и литературы должно соответствовать требованиям библиографических стандартов. Объем работы должен быть не менее 15 и не более 23 страниц. Работа должна выполняться через одинарный интервал, 14 шрифтом, страницы должны быть пронумерованы. Расстояние между названием части реферата или главы и последующим текстом должно быть равно трем интервалам. Каждая цитата должна сопровождаться ссылкой на источник, библиографическое описание которого должно приводиться в соответствии с требованиями библиографических стандартов. Оценивая реферат, преподаватель обращает внимание на соответствие содержания выбранной теме; соблюдение структуры работы. Учитывается умение работать с научной литературой - вычленять проблему из контекста; логически мыслить; оформлять научный текст (правильное применение и оформление ссылок, составление библиографии); умение правильно понять позицию авторов; соблюдение объема работы; аккуратность и правильность оформления. Реферат должен быть сдан для проверки в установленный срок

Приложение 1

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность и защита информации» реализуется кафедрой источниковедения.

Содержание дисциплины охватывает круг вопросов, связанных с информационной безопасностью и защитой информации в Российской Федерации.

Цель дисциплины: изучение теоретических и прикладных вопросов информационной безопасности и защиты информации в сфере документооборота и архивного дела в Российской Федерации.

Задачи дисциплины:

изучить исторические этапы развития информационной безопасности и защиты информации;

освоить терминологию и понятийный аппарат в области информационной безопасности и защиты информации;

изучить нормативно-правовую базу, регулирующую сферу информационной безопасности и защиты информации;

изучить основные средства и методы обеспечения информационной безопасности;

научить определять угрозы, уязвимости и риски информационной безопасности;

обучить навыкам защиты информации;

научить применять полученные знания и навыки по информационной безопасности и защите информации в сфере документооборота и архивного дела.

Дисциплина направлена на формирование следующих компетенций.

ПК- 4 - Способность создавать и вести системы документационного обеспечения управления архивов на базе новейших технологий

В результате освоения дисциплины обучающийся должен:

знать:

историю, современное состояние, проблемы и тенденции развития систем информационной безопасности и защиты информации;

нормативно-правовую базу обеспечения информационной безопасности и защиты информации;

систему органов власти, определяющих и реализующих государственную политику в области информационной безопасности и защиты информации;

систему документационного обеспечения информационной безопасности и защиты информации;

место и роль информационной безопасности и защиты информации в области документооборота и архивного дела;

методы и средства обеспечения информационной безопасности и защиты информации.

Уметь:

анализировать проблемы информационной безопасности и защиты информации в системах документооборота и архивном деле;

применять отечественные и зарубежные стандарты в области информационной безопасности и защиты информации;

определять угрозы, уязвимости и риски информационной безопасности; разрабатывать комплекс мер по обеспечению информационной безопасности и защиты информации в сфере документооборота и архивного дела.

Владеть:

терминологией и понятийным аппаратом в области информационной безопасности и защиты информации;

навыками использования методов и средств обеспечения информационной

безопасности и защиты информации;

навыками разработки документационного обеспечения безопасности и защиты информации.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме обзора, доклада, реферата, контрольной работы, опроса. Итоговая аттестация в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы.