

**МИНОБРНАУКИ РОССИИ**



Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«Российский государственный гуманитарный университет»  
(ФГБОУ ВО «РГГУ»)**

**ИСТОРИКО-АРХИВНЫЙ ИНСТИТУТ**

Факультет документоведения и технотронных архивов

Кафедра комплексной защиты информации ИИНТБ РГГУ

**Информационная безопасность и защита информации**

**Рабочая программа дисциплины**

Направление подготовки

**46.03.02 «Документоведение и архивоведение»**

Профиль подготовки

**Государственные и муниципальные архивы**

**Архивное дело за рубежом. История, культура и архивы Франции**

**Квалификация выпускника – бакалавр**

**Форма обучения – очная**

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Москва 2019

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Рабочая программа дисциплины

*Составитель:*

*...Петров Сергей Томасович*

*преподаватель кафедры КЗИ ФИСБ*

*Ответственный редактор:*

*Тарасов Александр Алексеевич*

*Заведующий кафедрой комплексной защиты информации, д.т.н., проф*

*Ларин Михаил Васильевич*

*заведующий кафедрой АС ДОУ, д.и.н., профессор*

**УТВЕРЖДЕНО**

*Протокол заседания кафедры КЗИ*

**№ 1 от 29.08.2019**

**ОГЛАВЛЕНИЕ**

**1. Пояснительная записка**

1.1 Цель и задачи дисциплины (*модуля*)

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (*модулю*)

1.3. Место дисциплины в структуре образовательной программы

**2. Структура дисциплины (*модуля*)****3. Содержание дисциплины (*модуля*)****4. Образовательные технологии****5. Оценка планируемых результатов обучения**

5.1. Система оценивания

5.2. Критерии выставления оценок

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

**6. Учебно-методическое и информационное обеспечение дисциплины**

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

**7. Материально-техническое обеспечение дисциплины (*модуля*)****8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья****9. Методические материалы**

9.1. Планы практических (семинарских, лабораторных) занятий

9.2. Методические рекомендации по подготовке письменных работ

9.3. Иные материалы

**Приложения**

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

### 1. Пояснительная записка

#### 1.1. Цель и задачи дисциплины

Содержание дисциплины охватывает круг проблем информационной безопасности и защиты информации в Российской Федерации.

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

Предметом изучения являются проблемы информационной безопасности и защиты информации в Российской Федерации, а также меры по их обеспечению в сфере документооборота и архивного дела.

Освоение дисциплины направлено на приобретение студентами знаний в области методов и средств обеспечения информационной безопасности, их использования в сфере документооборота и архивного дела.

#### **Задачи курса:**

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. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (модулю):

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОК-10	способность к использованию основных методов, способов и средств получения,	<i>Знать:</i> историю, современное состояние, проблемы и тенденции развития систем информационной безопасности и защиты

ОПК-6	<p>хранения, переработки информации способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>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;</p> <p>систему документационного обеспечения информационной безопасности и защиты информации; место и роль информационной безопасности и защиты информации в области документооборота и архивного дела;</p> <p>методы и средства обеспечения информационной безопасности и защиты информации.</p> <p><i>Уметь:</i></p> <p>анализировать проблемы информационной безопасности и защиты информации в системах документооборота и архивном деле;</p> <p>применять отечественные и зарубежные стандарты в области информационной безопасности и защиты информации;</p> <p>определять угрозы, уязвимости и риски информационной безопасности;</p> <p>разрабатывать комплекс мер по обеспечению информационной безопасности и защиты информации в сфере документооборота и архивного дела.</p> <p><i>Владеть:</i></p> <p>терминологией и понятийным аппаратом в области информационной безопасности и защиты информации;</p> <p>навыками использования методов и средств обеспечения информационной безопасности и защиты информации;</p> <p>навыками разработки документационного обеспечения информационной безопасности и защиты информации.</p>
-------	--	---

## 1.2. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность и защита информации» является частью обязательных дисциплин базовой части учебного плана профиля по направлению

«Информационно-документационное обеспечение управления» подготовки бакалавров 46.03.02 «Документоведение и архивоведение» и изучается на 6 семестре. Дисциплина реализуется на факультете Документоведения и технотронных архивов кафедрой Комплексной защиты информации ИИНТБ РГГУ.

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

Основы информационного общества (2 семестр);

Информатика (2 семестр);

Информационные технологии (3, 4 семестры);

Государственное регулирование деятельности коммерческих и некоммерческих организации РФ (4 семестр);

Информационное право (5 семестр).

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практик:

Конфиденциальное делопроизводство (6 семестр);

Защита и обработка персональных данных (7 семестр);

Защита конфиденциальной информации в кадровой службе (7 семестр);

Электронный документ и электронная подпись в законодательстве (8 семестр);

Информационные ресурсы организации (создание и использование) (8 семестр).

Нормативно-методические основы использования электронной подписи в ДОУ (9 семестр);

Обеспечение сохранности технотронных документов (9 семестр);

## 2. Структура дисциплины

### *Структура дисциплины для очной формы обучения*

Общая трудоемкость дисциплины для очной формы составляет 2 з. е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 час. (из них 12 лекции, 16 лабораторные), самостоятельная работа обучающихся 44 час.

№ 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)
				Лекции	Лабораторные занятия	Семинары	Самостоятельная работа	
1.	Введение	5						
2.	Раздел 1. Терминологический и	5		2	2		6	Доклад (эссе)

	понятийный аппарат ИБ и ЗИ							
3.	Раздел 2. Теоретические и прикладные основы ИБ и ЗИ	5		2	2		8	Реферат
4.	Раздел 3. Методы и средства обеспечения ИБ и ЗИ	5		2	4		8	Контрольная работа
5.	Раздел 4. Информационная безопасность Российской Федерации	5		2	4		8	Опрос
6.	Раздел 5. Документационное обеспечение ИБ и ЗИ	5		2	2		8	Контрольная работа (эссе)
7.	Раздел 6. Комплексная безопасность информационных активов	5		2	2		6	Опрос
8.	Итоговая аттестация	5		12	16		44	Зачет

### 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 обеспечения 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. Информационные и образовательные технологии

При реализации программы дисциплины используются различные образовательные и информационные технологии. Занятия проходят в классе, оснащенном компьютерами, подключенными к Интернет и объединенными в единую внутреннюю сеть ИАИ. Мобильные устройства обучающихся имеют выход в Интернет через wi-fi ИАИ. Занятия проходят с использованием ресурсов Интернет. Компьютеры оснащены одним из офисных пакетов и антивирусным средством.

Класс оснащен проекционным оборудованием и/или монитором для коллективного отображения информации.

Таблица 4. Использование информационных и образовательных технологий в ходе учебного процесса

<i>№ п/п</i>	<i>Наименование раздела</i>	<i>Виды учебной работы</i>	<i>Информационные и образовательные технологии</i>
1.	Введение	Лекция 1.  Самостоятельная работа	Вводная лекция с использованием Интернет-ресурсов  Подготовка доклада
2.	Раздел 1. Терминологический и понятийный аппарат ИБ и ЗИ	Лекция 2.  Лабораторная работа 1.  Самостоятельная работа	Проблемная 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	Лекция 4.	Проблемная лекция

	обеспечения ИБ и ЗИ	Лабораторная работа 3. Самостоятельная работа	Развернутая беседа с обсуждением контрольной работы Контрольная работа
5.	Раздел 4. Информационная безопасность Российской Федерации	Лекции 5 Лекция 6  Лабораторная работа 4.  Самостоятельная работа	Проблемные лекции 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

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания<sup>1</sup>

Система оценивания может быть представлена как в текстовой, так и в табличной форме.

Например:

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- участие в дискуссии на семинаре	5 баллов	30 баллов
- тест или реферат	30 баллов	30 баллов
Промежуточная аттестация		40 баллов
Зачёт		
<b>Итого за семестр (дисциплину)</b>		100 баллов
зачёт/зачёт с оценкой/экзамен		

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
--------------------	--------------------	------------

<sup>1</sup> Система оценивания выстраивается в соответствии с учебным планом, где определены формы промежуточной аттестации (зачёт/зачёт с оценкой/экзамен), и структурой дисциплины, где определены формы текущего контроля. Указывается распределение баллов по формам текущего контроля и промежуточной аттестации, сроки отчётности.

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<sup>2</sup>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>

<sup>2</sup> Могут уточняться и дополняться в соответствии со спецификой дисциплины, установленных форм контроля, применяемых технологий обучения и оценивания.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	«удовлетвори- тельно»/ «зачтено (удовлетвори- тельно)»/ «зачтено»	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворите- льно»/ не зачтено	<p>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.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

### 5.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности.

#### 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) основная литература*

1. Адрианов В.В. и др. Обеспечение информационной безопасности бизнеса. М., 2011.  
<https://new.znaniyum.com/catalog/document?id=135885>
2. Малюк А.А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах : учеб. пособие для студентов, обучающихся по

специальностям не входящим в группу специальностей в области информатики. М., 2011.

3. Некрах А.В. Шевцова Г.А. Организация конфиденциального делопроизводства и защита информации. М., 2007.

*б) дополнительная литература*

1. Бирюков А. А. Информационная безопасность: защита и нападение. М., 2013.
2. Галатенко В.А. Основы информационной безопасности : учеб. пособие : для студентов вузов, обучающихся по специальности «Прикладная информатика» / [под ред. В. Б. Бетелина]. М., 2008.
3. Ларин М.В., Янковая В.Ф. Организация хранения электронных документов // Современные технологии делопроизводства и документооборота. 2013, № 5.
4. Хорев П. Программно-аппаратная защита информации. Учебное пособие. М., 2015.  
<https://new.znaniyum.com/catalog/document?id=20764>

*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](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](http://www.cbr.ru/credit/gubzi_docs)
7. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт].  
<http://www.rsuh.ru/iintb>

## 7. Материально-техническое обеспечение дисциплины (модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, в том числе аудиторная доска (с магнитной поверхностью и набором приспособлений для крепления демонстрационных материалов), экран (на штативе или навесной), демонстрационный планшет с набором блокнотов для него и фломастеров. Для проведения практических занятий, а также организации самостоятельной работы студентов необходимы компьютерный класс с рабочими местами, обеспечивающими выход в Интернет, и программное обеспечение, позволяющее осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители. Кроме того, для информационно-ресурсного обеспечения практических занятий необходим доступ к сканеру, копировальному аппарату и принтеру.

Реализация программы обеспечивается доступом каждого студента к информационным ресурсам, распространяемым на цифровых носителях или по университетской локальной сети.

### Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2016 г.)

#### 1. Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 18 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Kaspersky Endpoint Security	Kaspersky	лицензионное

#### 2. Перечень БД и ИСС

Таблица 2

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2016 г. Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2016 г. Журналы Oxford University Press SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
4	Компьютерные справочные правовые системы

	Консультант Плюс, Гарант
--	-----------------------------

**Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)**

## 1. Перечень ПО

*Таблица 1*

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Office 2013	Microsoft	лицензионное

## 2. Перечень БД и ИСС

*Таблица 2*

№п/п	Наименование
1	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
2	Компьютерные справочные правовые системы Консультант Плюс, Гарант

## 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого от студента требуется представить заключение психолого-медико-педагогической комиссии (ПМПК) и личное заявление (заявление законного представителя).

В заключении ПМПК должно быть прописано:

- рекомендуемая учебная нагрузка на обучающегося (количество дней в неделю, часов в день);
- оборудование технических условий (при необходимости);
- сопровождение и (или) присутствие родителей (законных представителей) во время учебного процесса (при необходимости);
- организация психолого-педагогического сопровождение обучающегося с указанием специалистов и допустимой нагрузки (количества часов в неделю).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся при необходимости могут быть созданы фонды оценочных

средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

Форма проведения текущей и итоговой аттестации для лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно (на бумаге, на компьютере), в форме тестирования и т.п.). При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

## **9. Методические материалы<sup>3</sup>**

### **9.1. Планы семинарских занятий<sup>4</sup>**

#### **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):*

1. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года // Российская газета. 2009, 21 января.
2. Указ Президента Российской Федерации от 12 мая 2009 г. N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Российская газета. 2009, 19 мая.
3. Указ Президента Российской Федерации от 09 сентября 2000 г. N 1895 «О Доктрине информационной безопасности Российской Федерации» // Российская газета. 2009, 19 мая.
4. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212 // Российская газета. 2008, 16 февраля.

---

<sup>3</sup> Методические материалы по дисциплине могут входить в состав рабочей программы, либо разрабатываться отдельным документом.

<sup>4</sup> План занятий строится в соответствии со структурой дисциплины (п.2). Разделы плана включают: название темы, количество часов, форму проведения занятия, его содержание (вопросы для обсуждения, задания, контрольные вопросы, кейсы и т.п.), список литературы. При необходимости, планы практических и лабораторных занятий могут содержать указания по выполнению заданий и требования к материально-техническому обеспечению занятия.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М., 2007.

*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. Бабаш А., Елена Баранова Е., Ларин Д. Информационная безопасность. История защиты информации в России. М., 2013.
4. Бирюков А. А. Информационная безопасность: защита и нападение. М., 2013.  
Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. М., 2015.
5. Галатенко В.А. Основы информационной безопасности : учеб. пособие : для студентов вузов, обучающихся по специальности «Прикладная информатика» / [под ред. В. Б. Бетелина]. М., 2008.
6. Сохранение электронной информации в информационном обществе. Сборник материалов Международной конференции (Москва, 3 – 5 октября 2011 г.). М., 2011.
7. Тихонов В.И. Информационные технологии и электронные документы в контексте архивного дела (статьи разных лет). — М., 2009.
8. Хорев П. Программно-аппаратная защита информации. Учебное пособие. М., 2015.
9. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М., 2012.

## **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):*

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. N 149-ФЗ // Российская газета. 2006, 29 июля.
2. 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.
3. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014) . URL : <http://fstec.ru>. Дата обращения: 14.05.2015
4. [Методический документ]. Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов. М. Росархив, ВНИИДАД, 2012

*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 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 обеспечения 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):*

1. 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.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. М., 2007.
3. 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.
4. ГОСТ Р ИСО/МЭК 27003-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. М., 2007.
5. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012.
6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011.
7. ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013.
8. Об утверждении Состав 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

9. 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
10. [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/component/attachments/download/290> (дата обращения: 14.04.2015).
11. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014) . URL : <http://fstec.ru>. Дата обращения: 14.05.2015
12. [Методический документ]. Методические рекомендации по электронному копированию архивных документов и управлению полученным информационным массивом. М. Росархив, ВНИИДАД, 2012
13. [Методический документ]. Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов. М. Росархив, ВНИИДАД, 2012

*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. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года // Российская газета. 2009, 21 января.
2. Указ Президента Российской Федерации от 12 мая 2009 г. N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Российская газета. 2009, 19 мая.
3. Указ Президента Российской Федерации от 09 сентября 2000 г. N 1895 «О Доктрине информационной безопасности Российской Федерации» // Российская газета. 2009, 19 мая.
4. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212 // Российская газета. 2008, 16 февраля.
5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. N 149-ФЗ // Российская газета. 2006, 29 июля.
1. Об утверждении Составы 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

2. 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
3. [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/component/attachments/download/290> (дата обращения: 14.04.2015).
4. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014) . URL : <http://fstec.ru>. Дата обращения: 14.05.2015
5. [Методический документ]. Методические рекомендации по электронному копированию архивных документов и управлению полученным информационным массивом. М. Росархив, ВНИИДАД, 2012
6. [Методический документ]. Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов. М. Росархив, ВНИИДАД, 2012

*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 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):*

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. N 149-ФЗ // Российская газета. 2006, 29 июля.
2. О персональных данных: Федеральный закон от 29 июля 2006 г. N 152-ФЗ // Российская газета. 2006, 29 июля.
3. 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.
4. Об утверждении Составы 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
5. 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
6. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014) . URL : <http://fstec.ru>. Дата обращения: 14.05.2015

7. [Методический документ]. Методические рекомендации по электронному копированию архивных документов и управлению полученным информационным массивом. М. Росархив, ВНИИДАД, 2012
8. [Методический документ]. Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов. М. Росархив, ВНИИДАД, 2012

*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 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):*

1. Указ Президента Российской Федерации от 09 сентября 2000 г. N 1895 «О Доктрине информационной безопасности Российской Федерации» // Российская газета. 2009, 19 мая.
2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. N 149-ФЗ // Российская газета. 2006, 29 июля.
3. 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.
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М., 2007.
5. ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013.
6. 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
7. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014) . URL : <http://fstec.ru>. Дата обращения: 14.05.2015
8. [Методический документ]. Методические рекомендации по электронному копированию архивных документов и управлению полученным информационным массивом. М. Росархив, ВНИИДАД, 2012
9. [Методический документ]. Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов. М. Росархив, ВНИИДАД, 2012

*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.

### **АННОТАЦИЯ**

Дисциплина «Информационная безопасность и защита информации» является частью обязательных дисциплин цикла академической по направлению подготовки бакалавров 46.03.02 «Документоведение и архивоведение». Дисциплина реализуется на факультете Документоведения и электронных архивов кафедрой Комплексной защиты информации ИИНТБ РГГУ.

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.

*Общекультурные компетенции:*

способностью к использованию основных методов, способов и средств получения, хранения, переработки информации (ОК-10);

*Общепрофессиональные компетенции:*

способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6).

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 информационной 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.

*Общая трудоемкость освоения дисциплины составляет:* 2 зачетных единицы, 72 час.

*Приложение 2*

## ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	Приложение № 1	29.08.2019	1

*Приложение к листу изменений № 1*

УТВЕРЖДЕНО  
Протокол заседания кафедры  
№ 1 от 29.08.2019

### **ЛИСТ ИЗМЕНЕНИЙ**

в рабочей программе дисциплины Информационная безопасность и защита информации  
по направлению подготовки 46.03.02 Документоведение и архивоведение  
на 2019/2020 учебный год

1. Учебная дисциплина выведена из списка дисциплин учебного плана.

