

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

по направлению подготовки (специальности)

10.03.01 Информационная безопасность

по профилю:

Организация и технология защиты информации

Уровень квалификация выпускника - бакалавр

Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

Информационная безопасность в банковской сфере

Рабочая программа дисциплины

Составитель:

Кандидат технических наук, доцент,

доцент кафедры информационной безопасности Д.С. Карпов

Ответственный редактор

к.и.н., доцент, заведующая кафедрой

информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО

Протокол заседания кафедры информационной безопасности

№ 5 от 24.01.2017

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

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цели дисциплины: формирование у обучающихся навыков разработки и построения систем обеспечения информационной безопасности с учетом особенностей функционирования предприятий банковской отрасли путем раскрытия основных принципов, научно-методологической базы построения и особенностей организации системы обеспечения информационной безопасности в банковских организациях, как основных учреждениях кредитно-финансовой сферы.

Задачи дисциплины:

- изучение теоретических проблем выработки концепции построения системы обеспечения информационной безопасности в банковских организациях;
- изучение требований нормативных правовых актов, методических документов и отраслевых стандартов банковской отрасли по информационной безопасности;
- формирование практических навыков разработки структуры и архитектуры систем обеспечения информационной безопасности банковских организаций;
- формирование навыков определения состава ресурсообеспечения системы обеспечения информационной безопасности банковских организаций;
- формирование навыков разработки организационно-распорядительных документов по информационной безопасности в банковских организациях;
- выработка навыков самостоятельного применения методов анализа влияющих факторов и выбора средств для построения сложных систем, обеспечивающих информационную безопасность в банковских организациях.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	1) Знать: <ul style="list-style-type: none"> - основные подходы к организации и задачи защиты информации в организациях кредитно-финансовой сферы; - структуру, задачи и функции системы обеспечения информационной безопасности банковских организаций; - особенности правового регулирования деятельности по организации защиты информации в банковских организациях; 2) Уметь: <ul style="list-style-type: none"> - разрабатывать нормативно-методические и организационно-распорядительные документы, обеспечивающие процессы защиты различных категорий информации в организациях банковской сферы; - разрабатывать требования по обеспечению информационной безопасности банковских организаций и внедрять меры по их обеспечению; 3) Владеть: <ul style="list-style-type: none"> - методиками формирования перечней защищаемой информации; - навыками разработки требований к системе обеспечения информационной безопасности в банковских организациях на основе действующих отраслевых стандартов; - навыками эффективного внедрения мер по защите

		информации в существующие технологические процессы обработки информации в информационных системах банковских организаций
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	<p>1) Знать:</p> <ul style="list-style-type: none"> - структуру, задачи и функции системы обеспечения информационной безопасности банковских организаций; - особенности правового регулирования деятельности по организации защиты информации в банковских организациях; - состав угроз защищаемой информации в банковских организациях и методику их выявления, методику анализа и оценки рисков нарушения информационной безопасности банковских организаций, основы менеджмента рисков нарушения информационной безопасности <p>2) Уметь:</p> <ul style="list-style-type: none"> - разрабатывать требования по обеспечению информационной безопасности банковских организаций и внедрять меры по их обеспечению; - проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам. <p>3) Владеть:</p> <ul style="list-style-type: none"> - навыками разработки требований к системе обеспечения информационной безопасности в банковских организациях на основе действующих отраслевых стандартов; - навыками эффективного внедрения мер по защите информации в существующие технологические процессы обработки информации в информационных системах банковских организаций
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной	<p>1) Знать:</p> <ul style="list-style-type: none"> - особенности правового регулирования деятельности по организации защиты информации в банковских организациях; - состав угроз защищаемой информации в банковских организациях и методику их выявления, методику анализа и оценки рисков нарушения информационной безопасности банковских организаций, основы менеджмента рисков нарушения информационной безопасности; - требования к системе защиты информации учреждений и предприятий банковской сферы и методы оценки их соблюдения. <p>2) Уметь:</p> <ul style="list-style-type: none"> - проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам. <p>3) Владеть:</p> <ul style="list-style-type: none"> - навыками эффективного внедрения мер по защите информации в существующие технологические процессы обработки информации в информационных системах

	службы по техническому и экспортному контролю	банковских организаций; - навыками выработки рекомендаций по составу организационно-технических мер по защите информации в банковских организациях, направленных на повышение защищенности их информационных; - методикой оценки соответствия действующей в банковской организации системы обеспечения информационной безопасности требованиям отраслевых стандартов.
--	---	---

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность в банковской сфере» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Основы информационной безопасности, Организационное обеспечение информационной безопасности, Правовое обеспечение информационной безопасности, Специальные нормативные документы и стандарты по информационной безопасности, Основы управления информационной безопасностью, Системы управления информационной безопасностью, Управление информационными рисками.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: Комплексное обеспечение безопасности объекта информатизации, преддипломная практика.

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 44 ч.

№ п/ п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельна я работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (<i>по семестрам</i>)
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточна я аттестация		
1	Структура учреждений и предприятий банковской сферы. Место защиты информации в деятельности учреждений и предприятий банковской сферы	8	4		2			7	Участие в дискуссии на практическом занятии, опрос
2	Принципы и	8	2		2			7	Участие в

	методика выявления состава защищаемой информации банковских организаций								дискуссии на практическом занятии, опрос, выступление с докладом
3	Основные подходы к анализу и оценке рисков нарушения информационной безопасности банковских организаций	8	2		2			7	Участие в дискуссии на практическом занятии, опрос
4	Общий концептуальный подход к обеспечению информационной безопасности банковских организаций. Взаимосвязь и содержание понятий «система обеспечения информационной безопасности», «система информационной безопасности», «система менеджмента информационной безопасности».	8	4		2			9	Участие в дискуссии на практическом занятии, опрос, выступление с докладом
5	Нормативно-методическое обеспечение деятельности службы защиты информации в банковских организациях	8	2		2			7	Участие в дискуссии на практическом занятии, опрос
6	Проведение контроля функционирования системы защиты информации. Внутренний и внешний аудит информационной безопасности.	8	2		2			7	Участие в дискуссии на практическом занятии, тестирование
	зачёт	8							Зачет по

								<i>вопросам билетов</i>
	ИТОГО:		16		12			44

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Структура учреждений и предприятий банковской сферы. Место защиты информации в деятельности учреждений и предприятий банковской сферы	Предмет, содержание, цели и задачи изучения дисциплины. Назначение дисциплины и ее место в подготовке специалистов в области ИБ. Структура банковской системы РФ. Банки как основа кредитно-финансовой отрасли экономики. Основные виды современных банков (ипотечные, инвестиционные, сберегательные и т.п.), их цели, задачи, функции. Специфика деятельности банков. Информация и информационные процессы в структуре банковской деятельности. Особенности технологии обработки информации в банковских информационных системах. Безопасность как основа функционирования предприятий данной сферы деятельности. Значение организации эффективной защиты информации в деятельности банковских организаций. Особенности защиты информации в организациях банковской сферы.
2.	Принципы и методика выявления состава защищаемой информации банковских организаций	Состав защищаемой информации в банковских организациях. Понятие «банковская тайна», ее отличительные особенности и взаимосвязь с такими видами тайны как, «семейная тайна», «личная тайна», «персональные данные». Субъекты банковской тайны. Понятие «коммерческая тайна банка», ее взаимосвязь и соотношение с банковской тайной. Критерии отнесения информации к коммерческой тайне банка и банковской тайне. Назначение, структура и технология формирования перечня защищаемой информации. Правовые основы создания перечня сведений, составляющих коммерческую тайну банковской организации. Функции руководства, основных подразделений кредитного учреждения и должностных лиц по разработке данного перечня сведений. Персональные данные, как отдельная категория защищаемых информационных ресурсов банковской организации.
3.	Основные подходы к анализу и оценке рисков нарушения информационной безопасности банковских организаций	Банковские риски: определение понятия, классификация банковских рисков и их связь с угрозами защищаемой информации и рисками нарушения информационной безопасности. Понятия «модель угроз» и «модель нарушителя», их содержание и особенности формирования. Основные подходы к анализу, оценке и обработке

		рисков нарушения информационной безопасности.
4.	Общий концептуальный подход к обеспечению информационной безопасности банковских организаций. Взаимосвязь и содержание понятий «система обеспечения информационной безопасности», «система информационной безопасности», «система менеджмента информационной безопасности».	<p>Сущность концепции построения систем обеспечения информационной безопасности в банковских организациях. Понятие «политики безопасности». Понятие «системы обеспечения информационной безопасности» банковских организаций.</p> <p>Основные цели, задачи и подходы к организации комплексной системы защиты информации в банковских структурах. Процедура формирования архитектуры комплексной системы защиты информации в банке. Взаимосвязь понятий «система информационной безопасности» и «комплексная система защиты информации». Основные группы требований к системе ИБ.</p> <p>Процессный подход к управлению, его сущность и содержание. Понятие системы менеджмента информационной безопасности и требования к ней. Функции, задачи и особенности деятельности службы защиты информации банковской организации. Права, обязанности и ответственность сотрудников службы защиты информации банка.</p>
5.	Нормативно-методическое обеспечение деятельности службы защиты информации в банковских организациях	<p>Структура внутренних документов банковских организаций по обеспечению информационной безопасности. Уровни «пирамиды» документации по информационной безопасности. Документы, содержащие положения корпоративной политики информационной безопасности. Частные политики безопасности второго уровня. Документы, содержащие требования информационной безопасности и процедуры (инструктивные и регламентные документы). Документы, содержащие свидетельства выполненной деятельности по информационной безопасности. Требования к документированию процессов защиты информации, особенности формирования документации, ее необходимость для проведения аудита ИБ.</p>
6.	Проведение контроля функционирования системы защиты информации. Внутренний и внешний аудит информационной безопасности.	<p>Понятие контроля, как необходимого звена процессов управления системой информационной безопасности в банковских организациях. Понятия «самооценка», «внутренний аудит», «внешний аудит» и их соотношение. Методика проведения аудита информационной безопасности банковских организаций. Рекомендуемые уровни зрелости процессов менеджмента информационной безопасности, их характеристика и связь с процессами контроля и аудита ИБ.</p>

4. Образовательные технологии

№	Наименование	Виды учебных	Образовательные технологии
---	--------------	--------------	----------------------------

п/п	раздела	занятий	
1	2	3	4
1.	Структура учреждений и предприятий банковской сферы. Место защиты информации в деятельности учреждений и предприятий банковской сферы	Лекция 1. Практическое занятие 1. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты
2.	Принципы и методика выявления состава защищаемой информации банковских организаций	Лекция 2. Практическое занятие 2. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Выступления с докладами. Консультирование и проверка домашних заданий посредством электронной почты
3.	Основные подходы к анализу и оценке рисков нарушения информационной безопасности банковских организаций	Лекция 3. Практическое занятие 3. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Консультирование и проверка домашних заданий посредством электронной почты
4.	Общий концептуальный подход к обеспечению информационной безопасности банковских организаций. Взаимосвязь и содержание понятий «система обеспечения информационной безопасности», «система информационной безопасности», «система менеджмента информационной безопасности».	Лекция 4. Практическое занятие 4. Самостоятельная работа	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции. Опрос. Выступления с докладами. Консультирование и проверка домашних заданий посредством электронной почты
5.	Нормативно-методическое обеспечение	Лекция 5. Практическое	Лекция с использованием видеоматериалов Развернутая беседа с обсуждением лекции.

	деятельности службы защиты информации в банковских организациях	<p><i>занятие 5.</i></p> <p><i>Самостоятельная работа</i></p>	<p><i>Опрос.</i></p> <p><i>Консультирование и проверка домашних заданий посредством электронной почты</i></p>
6.	<p>Проведение контроля функционирования системы защиты информации. Внутренний и внешний аудит информационной безопасности.</p>	<p><i>Лекция 6.</i></p> <p><i>Практическое занятие 6.</i></p> <p><i>Самостоятельная работа</i></p>	<p><i>Лекция с использованием видеоматериалов</i></p> <p><i>Развернутая беседа с обсуждением лекции. Тестирование.</i></p> <p><i>Консультирование и проверка домашних заданий посредством электронной почты</i></p>

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос пр. занятия	4 балла	20 баллов
- участие в дискуссии на пр. занятии	3 балла	18 баллов
- выступление с докладом	6 баллов	12 баллов
- тестирование	10 баллов	10 баллов
Промежуточная аттестация (зачет)		40 баллов
Итого за семестр (дисциплину)		100 баллов

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	1-3	ОПК-7, ПК-13	- оценка по итогам опроса на пр. занятии - оценка по итогам участия в дискуссии на пр. занятии - оценка выступления с докладом - тестирование
2.	4-7	ОПК-7, ПК-13, ПК-15	

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/ А,В	«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. 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/ С	«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>
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</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p> <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. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль (вариант опросного задания)

Вопросы	Реализуемая компетенция
1. Понятие информационной безопасности	ОПК-7
2. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?	ПК-13
3. Что такое политика СУИБ?	ПК-15

Текущий контроль (вариант теста) – проверка сформированности компетенций — ОПК-7, ПК-13, ПК-15

- 1) **К кредитным организациям относятся:**
 - a) банки и небанковские кредитные организации
 - b) только банки
 - c) банки, небанковские кредитные организации, аудиторские организации
- 2) **В состав банковской тайны входят:**
 - a) сведения о доходах и расходах банковской организации, сведения о количестве и суммах сделок с ценными бумагами
 - b) сведения о клиентах банка, о счетах и вкладах клиентов банка, об операциях по счетам
 - c) сведения о клиентах банка, персональные данные работников банка, сведения об обеспечении безопасности банковской организации
- 3) **Сведения, составляющие банковскую тайну, могут быть предоставлены:**

- a) только клиентам банковской организации, к которым относятся данные сведения
- b) любой организации или частному лицу по письменному запросу
- c) клиентам банковской организации, к которым относятся данные сведения, а также уполномоченным государственным органам и их должностным лицам и иным организациям, перечень которых установлен законом
- 4) **Банковская организация является оператором:**
 - a) персональных данных клиентов банковской организации и ее работников
 - b) персональных данных только работников банковской организации
 - c) банковские организации не являются операторами персональных данных
- 5) **Банковский риск – это:**
 - a) вероятность ухудшения состояния экономики государства вследствие нарушения функционирования банковской системы
 - b) вероятность несения кредитной организацией потерь вследствие наступления неблагоприятных событий, связанных с внутренними и (или) внешними факторами
 - c) вероятность несения клиентами банковской организации убытков вследствие ухудшения экономической обстановки в государстве и мире
- 6) **Риск возникновения у кредитной организации убытков вследствие несоблюдения кредитной организацией требований нормативных правовых актов и заключенных договоров – это:**
 - a) правовой риск
 - b) операционный риск
 - c) кредитный риск
- 7) **Риск нарушения информационной безопасности – это:**
 - a) риск, связанный с угрозой информационной безопасности
 - b) риск, связанный с выполнением банковских операций
 - c) риск, связанный с наличием денежных средств на счетах банковской организации
- 8) **Оценка риска нарушения информационной безопасности проводится на основании сопоставления оценок:**
 - a) степени возможности реализации угроз информационной безопасности и степени тяжести последствий от потери значимых свойств информационной безопасности
 - b) стоимости активов банковской организации и объема финансовых ресурсов, выделяемых на обеспечение информационной безопасности
 - c) количества источников угроз информационной безопасности и количества используемых средств защиты информации
- 9) **Для итогового оценивания рисков используется следующая шкала:**
 - a) допустимый и недопустимый риск
 - b) минимальный и максимальный риск
 - c) качественный и количественный риск
- 10) **Значимыми свойствами информационной безопасности, определяемыми в ходе реализации процедур оценки рисков нарушения информационной безопасности, являются:**
 - a) конфиденциальность, целостность, доступность информации
 - b) важность, ценность, объем информации
 - c) стоимость, сложность, число компонентов системы информационной безопасности

Примерные темы докладов - проверка сформированности компетенций **ОПК-7, ПК-13, ПК-15**

1. Подбор персонала по информационной безопасности в организации банковской системы Российской Федерации - ОПК-7, ПК-13
2. Особенности аудита информационной безопасности организаций банковской системы Российской Федерации - ПК-13, ПК-15

3. Правоприменительная практика в сфере информационно-компьютерных технологий Банковской системы РФ - ОПК-7, ПК-15
4. Рекомендации от ФинЦЕРТ для граждан и кредитных организаций - ОПК-7, ПК-13
5. Стандарты Банка России по информационной безопасности - ПК-13, ПК-15
6. Обзор крупнейших атак организаций банковской системы Российской Федерации за последние годы - ОПК-7, ПК-15
7. Риски и конфликты в банковской сфере - ОПК-7, ПК-13
8. Нормативно-правовая база обеспечения информационной безопасности в банковской сфере - ПК-13, ПК-15
9. Международные стандарты информационной безопасности в банковской сфере - ОПК-7, ПК-15
10. Методы противодействия основным угрозам информационной безопасности в финансовой сфере - ОПК-7, ПК-13

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций - ОПК-7, ПК-13, ПК-15

1. Краткая характеристика истории развития и современное состояние кредитно-финансовой системы в Российской Федерации.
2. Центральный банк Российской Федерации.
3. Ассоциация российских банков
4. Структура банковской системы Российской Федерации.
5. Банки как основа кредитно-финансовой отрасли экономики.
6. Основные виды современных банков (ипотечные, инвестиционные, сберегательные и т.п.), их цели, задачи, функции. Специфика деятельности банков.
7. Информация и информационные процессы в структуре банковской деятельности.
8. Особенности технологии обработки информации в банковских информационных системах.
9. Безопасность как основа функционирования предприятий банковской сферы.
10. Значение организации эффективной защиты информации в деятельности банковских организаций.
11. Особенности защиты информации в организациях банковской сферы.
12. Состав защищаемой информации в банковских организациях.
13. Понятие «банковская тайна», ее отличительные особенности и взаимосвязь с такими видами тайны как, «семейная тайна», «личная тайна», «персональные данные».
14. Субъекты банковской тайны.
15. Понятие «коммерческая тайна банка», ее взаимосвязь и соотношение с банковской тайной.
16. Критерии отнесения информации к коммерческой тайне банка и банковской тайне.
17. Назначение, структура и технология формирования перечня защищаемой информации.
18. Правовые основы создания перечня сведений, составляющих коммерческую тайну банковской организации.
19. Функции руководства, основных подразделений кредитного учреждения и должностных лиц по разработке данного перечня сведений.
20. Персональные данные, как отдельная категория защищаемых информационных ресурсов банковской организации.
21. Банковские риски: определение, классификация банковских рисков и их связь с угрозами защищаемой информации и рисками нарушения информационной безопасности.
22. Понятия «модель угроз» и «модель нарушителя», их содержание и особенности формирования.

23. Основные подходы к анализу, оценке и обработке рисков нарушения информационной безопасности.
24. Сущность концепции построения систем обеспечения информационной безопасности в банковских организациях, современные подходы и стандарты в области обеспечения информационной безопасности в организациях банковской системы.
25. Понятие «политики безопасности», ее цели, назначение и основное содержание.
26. Понятие «системы обеспечения информационной безопасности» банковских организаций.
27. Взаимосвязь понятий «система обеспечения информационной безопасности», «система информационной безопасности», «система менеджмента информационной безопасности».
28. Основные цели, задачи и подходы к организации комплексной системы защиты информации в банковских структурах.
29. Процедура формирования архитектуры комплексной системы защиты информации в банке.
30. Взаимосвязь понятий «система информационной безопасности» и «комплексная система защиты информации».
31. Основные группы требований к системе информационной безопасности.
32. Управление процессами обеспечения информационной безопасности банковских организаций. Система менеджмента информационной безопасности.
33. Процессный подход к управлению, его сущность и содержание. Процессы, формирующие управленческий цикл.
34. Понятие системы менеджмента информационной безопасности. Основные требования к системе менеджмента информационной безопасности и их взаимосвязь с процессами управления.
35. Функции, задачи и особенности деятельности службы защиты информации банковской организации.
36. Права, обязанности и ответственность сотрудников службы защиты информации банка.
37. Типы организационных структур банковских организаций.
38. Основные категории работников банковских организаций, проблемы их взаимодействия со специалистами службы защиты информации.
39. Профессиональные требования, предъявляемые к сотрудникам службы защиты информации в банковских организациях.
40. Особенности изучения и проверки кандидатов для работы в службе защиты информации банковских организаций.
41. Нормативно-методическое обеспечение деятельности службы защиты информации в банковских организациях.
42. Структура внутренних документов банковских организаций по обеспечению информационной безопасности.
43. Уровни «пирамиды» документации по информационной безопасности.
44. Документы, содержащие положения корпоративной политики информационной безопасности. Частные политики безопасности второго уровня.
45. Документы, содержащие требования информационной безопасности и процедуры (инструктивные и регламентные документы).
46. Документы, содержащие свидетельства выполненной деятельности по информационной безопасности.
47. Требования к документированию процессов защиты информации, особенности формирования документации, ее необходимость для проведения аудита информационной безопасности.

48. Понятие контроля, как необходимого звена процессов управления системой информационной безопасности в банковских организациях. Понятия «самооценка», «внутренний аудит», «внешний аудит» и их соотношение.
49. Методика проведения аудита информационной безопасности банковских организаций
50. Рекомендуемые уровни зрелости процессов менеджмента информационной безопасности, их характеристика и связь с процессами контроля и аудита информационной безопасности.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основная литература

а) основная:

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/612572>, свободный. — Загл. с экрана. — Яз. рус.
2. Банковский риск-менеджмент: Учебное пособие / П.П. Ковалев. - 2-е изд., перераб. и доп. - М.: КУРС: НИЦ ИНФРА-М, 2013. - 320 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/411068>, свободный. — Загл. с экрана. — Яз. рус.
3. Банковское дело: организация деятельности центрального банка и коммерческого банка, небанковских организаций : учебник / А.А. Казимагомедов. – М. : ИНФРА-М, 2017. – 502 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/759928>, свободный. — Загл. с экрана. — Яз. рус.

б) Дополнительная литература

4. Банковские системы: Учебное пособие / С.А. Андрюшин; Финансовая Академия при Правительстве РФ. - М.: Альфа-М: НИЦ Инфра-М, 2013. - 384 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/371307>, свободный. — Загл. с экрана. — Яз. рус.
5. Международно-правовые стандарты регулирования банковской деятельности / А.С. Линников, Л.К. Карпов. - М.: Статут, 2014. - 173 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/493002>, свободный. — Загл. с экрана. — Яз. рус.
6. Банковское право Российской Федерации: Учебное пособие / Отв. ред. Е.Ю. Грачева. - 2-е изд., перераб. и доп. - М.: Норма: НИЦ Инфра-М, 2016. - 400 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/549829>, свободный. — Загл. с экрана. — Яз. рус.
7. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стереотип. – М.: Флинта, 2011. – 269 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/453734>, свободный. — Загл. с экрана. — Яз. рус.

в) Информационно-справочная литература

9. Банковское дело: словарь официальных терминов с комментариями / Тавасиев А.М., Алексеев Н.К., - 2-е изд. - М.: Дашков и К, 2017. - 656 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/513901>, свободный. — Загл. с экрана. — Яз. рус.

10. Банковские технологии и преступность / Шмонин А.В. - М.:ЮНИТИ-ДАНА, 2015. - 303 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/859088>, свободный. — Загл. с экрана. — Яз. рус.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Центральный банк Российской Федерации [Электронный ресурс] — Режим доступа: <http://www.cbr.ru>, свободный. — Загл. с экрана. — Яз. рус., англ.
2. Федеральный портал по научной и инновационной деятельности [Электронный ресурс] — Режим доступа: <http://www.sci-innov.ru>, свободный. — Загл. с экрана. — Яз. рус., англ.
3. Научная электронная библиотека eLibrary [Электронный ресурс] — Режим доступа: <http://www.elibrary.ru>, свободный. — Загл. с экрана. — Яз. рус., англ.
4. Росстандарт. Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] — Режим доступа: <http://www.gost.ru>, свободный. — Загл. с экрана. — Яз. рус., англ.
5. Консультант плюс [Электронный ресурс] — Режим доступа: <http://www.consultant.ru>, свободный. — Загл. с экрана. — Яз. рус., англ.

6.3. Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Перечень ПО

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации

в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

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, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - проверка сформированности компетенций - ОПК-7, ПК-13, ПК-15

Практическое занятие:

Тема 1 (2 ч.) (Структура учреждений и предприятий банковской сферы. Место защиты информации в деятельности учреждений и предприятий банковской сферы) - **проверка сформированности компетенций - ОПК-7, ПК-13**

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу.

Список литературы:

[1, 3, 5] (см. Подраздел 6.1), [1] (см. Подраздел 6.2)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 2 (2 ч.) (Принципы и методика выявления состава защищаемой информации банковских организаций) - **проверка сформированности компетенций - ОПК-7, ПК-13**

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
3. Выступления с докладами.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
3. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.

Список литературы:

[1, 2, 4] (см. Подраздел 6.1)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 3 (2 ч.) (Основные подходы к анализу и оценке рисков нарушения информационной безопасности банковских организаций) - **проверка сформированности компетенций - ОПК-7, ПК-13**

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.

Список литературы:

[2, 7, 10] (см. Подраздел 6.1)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 4 (2 ч.) (Общий концептуальный подход к обеспечению информационной безопасности банковских организаций. Взаимосвязь и содержание понятий «система обеспечения информационной безопасности», «система информационной безопасности», «система менеджмента информационной безопасности») - **проверка сформированности компетенций ПК-13, ПК-15**

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
3. Выступления с докладами.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
3. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.

Список литературы:

[1, 4, 5, 11] (см. Подраздел 6.1)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 5 (2 ч.) (Нормативно-методическое обеспечение деятельности службы защиты информации в банковских организациях)- **проверка сформированности компетенций ПК-13, ПК-15**

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.

Список литературы:

[3, 6, 7, 11] (см. Подраздел 6.1), [4] (см. Подраздел 6.2)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:

Тема 6 (2 ч.) (Проведение контроля функционирования системы защиты информации. Внутренний и внешний аудит информационной безопасности) - **проверка сформированности компетенций ОПК-7, ПК-15**

Задания:

1. Дискуссия по обсуждению вопросов лекции.
2. Тестирование по дисциплине.

Указания по выполнению заданий:

1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы теста по курсу дисциплины.

Список литературы:

[1, 6, 7, 8] (см. Подраздел 6.1)

Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность в банковской сфере» реализуется на *факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедры информационной безопасности.*

Цели дисциплины: формирование у обучающихся навыков разработки и построения систем обеспечения информационной безопасности с учетом особенностей функционирования предприятий банковской отрасли путем раскрытия основных принципов, научно-методологической базы построения и особенностей организации системы обеспечения информационной безопасности в банковских организациях, как основных учреждениях кредитно-финансовой сферы.

Задачи:

- изучение теоретических проблем выработки концепции построения системы обеспечения информационной безопасности в банковских организациях;
- изучение требований нормативных правовых актов, методических документов и отраслевых стандартов банковской отрасли по информационной безопасности;
- формирование практических навыков разработки структуры и архитектуры систем обеспечения информационной безопасности банковских организаций;
- формирование навыков определения состава ресурсообеспечения системы обеспечения информационной безопасности банковских организаций;
- формирование навыков разработки организационно-распорядительных документов по информационной безопасности в банковских организациях;
- выработка навыков самостоятельного применения методов анализа влияющих факторов и выбора средств для построения сложных систем, обеспечивающих информационную безопасность в банковских организациях..

Дисциплина (модуль) направлена на формирование следующих компетенций:

ОПК-7 (*способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты*);

ПК-13 (*способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации*);

ПК-15 (*способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю*).

В результате освоения дисциплины (модуля) обучающийся должен:

1) Знать:

- основные подходы к организации и задачи защиты информации в организациях кредитно-финансовой сферы;
- структуру, задачи и функции системы обеспечения информационной безопасности банковских организаций;
- особенности правового регулирования деятельности по организации защиты информации в банковских организациях;
- состав угроз защищаемой информации в банковских организациях и методику их выявления, методику анализа и оценки рисков нарушения информационной безопасности

банковских организаций, основы менеджмента рисков нарушения информационной безопасности;

- требования к системе защиты информации учреждений и предприятий банковской сферы и методы оценки их соблюдения.

2) Уметь:

- разрабатывать нормативно-методические и организационно-распорядительные документы, обеспечивающие процессы защиты различных категорий информации в организациях банковской сферы;

- разрабатывать требования по обеспечению информационной безопасности банковских организаций и внедрять меры по их обеспечению;

- проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам.

3) Владеть:

- методиками формирования перечней защищаемой информации;

- навыками разработки требований к системе обеспечения информационной безопасности в банковских организациях на основе действующих отраслевых стандартов;

- навыками эффективного внедрения мер по защите информации в существующие технологические процессы обработки информации в информационных системах банковских организаций;

- навыками выработки рекомендаций по составу организационно-технических мер по защите информации в банковских организациях, направленных на повышение защищенности их информационных;

- методикой оценки соответствия действующей в банковской организации системы обеспечения информационной безопасности требованиям отраслевых стандартов.

По дисциплине предусмотрена промежуточная аттестация в форме *зачета*.

Общая трудоемкость освоения дисциплины (модуля) составляет 2 зачетные единицы, 72 часа.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.06.2017 г.	10
2	<i>Обновлена основная и дополнительная литература</i>	26.06.2018 г.	20
3	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	26.06.2018 г.	20
4	<i>Обновлена основная и дополнительная литература</i>	29.08.2019 г.	1
5	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.08.2019 г.	1
6	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)</i>	23.06.2020 г	14
7	<i>Обновлена основная и дополнительная литература</i>	23.06.2020 г	14
8	<i>Обновлен раздел п.4 Образовательные технологии</i>	23.06.2020 г	14
9	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	23.06.2020 г	14

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

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

*Кандидат технических наук, доцент,
доцент кафедры информационной безопасности Д.С. Карпов*

2. Обновление основной и дополнительной литературы (2018 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел *Дополнительная литература*

Информационные технологии в финансово-банковской сфере / Вдовин В.М., Суркова Л.Е. - М.: Дашков и К, 2018. - 304 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/450752>, свободный. — Загл. с экрана. — Яз. рус.

Дополнить раздел *Информационно-справочная литература*

Искусство управления информационными рисками / Астахов А.М., - 2-е изд., (эл.) - М.: ДМК Пресс, 2018. - 314 с. [Электронный ресурс] — Режим доступа: <http://znanium.com/catalog/product/220885>, свободный. — Загл. с экрана. — Яз. рус.

3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2018 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 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г.

	Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

Кандидат технических наук, доцент,

доцент кафедры информационной безопасности Д.С. Карпов

4. Обновление основной и дополнительной литературы (2019 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел *Дополнительная литература*

Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — www.dx.doi.org/10.12737/11380. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1009606>

5. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)**Перечень ПО**

№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 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

2. Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной

	подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

Кандидат технических наук, доцент,

доцент кафедры информационной безопасности Д.С. Карпов

6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)**Структура дисциплины (модуля) для очной формы обучения**

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 48 ч.

№ п/ п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (<i>по семестрам</i>)
			контактная					Самостоятельна я работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточна я аттестация		
1	Структура учреждений и предприятий банковской сферы. Место защиты информации в деятельности учреждений и предприятий банковской сферы	8	4		2			8	Участие в дискуссии на практическом занятии, опрос
2	Принципы и методика выявления состава защищаемой информации банковских организаций	8	2		2			8	Участие в дискуссии на практическом занятии, опрос, выступление с докладом
3	Основные подходы к анализу и оценке рисков нарушения информационной безопасности банковских организаций	8	2		2			8	Участие в дискуссии на практическом занятии, опрос
4	Общий концептуальный подход к обеспечению информационной безопасности банковских организаций. Взаимосвязь и содержание	8	4		2			8	Участие в дискуссии на практическом занятии, опрос, выступление с докладом

	понятий «система обеспечения информационной безопасности», «система информационной безопасности», «система менеджмента информационной безопасности».								
5	Нормативно-методическое обеспечение деятельности службы защиты информации в банковских организациях	8	2		2			8	Участие в дискуссии на практическом занятии, опрос
6	Проведение контроля функционирования системы защиты информации. Внутренний и внешний аудит информационной безопасности.	8	2		2			8	Участие в дискуссии на практическом занятии, тестирование
	зачёт	8							Зачет по вопросам билетов
	ИТОГО:		16		12			48	

7. Обновление основной и дополнительной литературы (2020 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел **Основная литература**

Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 336 с. — (Высшее образование). - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1114032>

Дополнить раздел **Дополнительная литература**

Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2020. — 223 с. - ISBN 978-5-16-015718-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1048121>

8. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

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.

9. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Состав программного обеспечения (ПО)

№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 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

К.и.н, доцент, Г.А. Шевцова