

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 Защита информации в банковских системах

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Квалификация выпускника специалист

Форма обучения очная

1. Цели освоения дисциплины:

- формирование у студентов системы знаний в области обеспечения информационной безопасности банковской деятельности;
- изучение основных положений концепции и политики безопасности банковских систем;
- изучение основных методов анализа состояния безопасности банковской системы и роли защиты информации в ее обеспечении;
- изучение угроз безопасности банков и основных преступлений в банковской сфере;
- изучение основных подходов к созданию системы безопасности банков и особенностей ее функционирования;
- изучение особенностей аудита банковской безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в банковских системах» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Защита информации в банковских системах» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-4 ПК-4	Моделирование систем Основы информационной безопасности
ПК-6	Организация ЭВМ и вычислительных систем

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-4, ПК-6	Защита информации в телекоммуникационных системах
ПК-6	Экономика и менеджмент в информационной безопасности критически важных объектов
ПК-4, ПК-6	Производственная научно-исследовательская работа
ПК-4, ПК-6	Производственная (преддипломная) практика
ПК-4, ПК-6	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Этап 1: Угрозы безопасности и методы защиты информации в банковских информационных системах	Этап 1: Выявлять угрозы системе безопасности банка и разрабатывать комплекс мер по ее совершенствованию	Этап 1: Оценки эффективности систем защиты информации банковских систем
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Этап 2: Основные правила разработки политики безопасности организации. Компоненты политики безопасности	Этап 2: Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;	Этап 2: Навыки применения комплексного подхода к обеспечению информационной безопасности банковских систем
ПК-6 - Способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Этап 1: Общие принципы организации безопасности банковских систем	Этап 1: Уметь анализировать информацию, возникающую в процессе деятельности банка, вырабатывать рекомендации целесообразности ее защиты.	Этап 1: Навыки выявления угроз в системе безопасности банка и разработки комплекс мер по ее совершенствованию
ПК-6 - Способностью проводить анализ, предлагать и	Этап 2: Угрозы безопасности и	Этап 2: Уметь проводить анализ и выбор	Этап 2: Использовать существующие

<p>обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p>	<p>методы защиты информации в банковских информационных системах</p>	<p>автоматизированные системы с целью обеспечения безопасности банковской информации</p>	<p>автоматизированные системы с целью совершенствования системы защиты банка</p>
--	--	--	--

4. Объем дисциплины

Объем дисциплины «Защита информации в банковских системах» составляет 5 зачетных единиц (180 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 8	
				КР	СР
1	2	3	4	5	6
1	Лекции (Л)	38		38	
2	Лабораторные работы (ЛР)	38		38	
3	Практические занятия (ЛР)				
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИБ)		40		40
10	Подготовка к занятиям (ПкЗ)		60		60
11	Промежуточная аттестация	4		4	
12	Наименование вида промежуточной аттестации	х	х	экзамен	
13	Всего	80	100	80	100

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций	
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	
1.	Раздел 1 Концепция безопасности банковских систем	8	10	10					x		10	14	x	ПК-4, ПК-6
1.1.	Тема 1 Основные положения концепции безопасности банка	8	6	6					x		6	8	x	ПК-4, ПК-6
1.2.	Тема 2 Политика безопасности	8	4	4					x		4	6	x	ПК-4, ПК-6
2.	Раздел 2 Угрозы безопасности банка	8	10	10					x		10	16	x	ПК-4, ПК-6
2.1.	Тема 3 Классификация угроз. Матрица угроз	8	6	6					x		6	8	x	ПК-4, ПК-6
2.2.	Тема 4 Мошенничество. Виды мошенничества	8	4	4					x		4	8	x	ПК-4, ПК-6
3.	Раздел 3 Основы информационной безопасности автоматизированных банковских систем	8	10	10					x		10	16	x	ПК-4, ПК-6

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
3.1.	Тема 5 Общие принципы обеспечения безопасности в автоматизированных банковских системах	8	4	6				x		4	8	x	ПК-4, ПК-6
3.2.	Тема 6 Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	8	6	4				x		6	8	x	ПК-4, ПК-6
4.	Раздел 4 Система безопасности банка	8	8	8				x		10	14	x	ПК-4, ПК-6
4.1.	Тема 7 Организация и функционирование системы безопасности банка	8	4	4				x		6	8	x	ПК-4, ПК-6
4.2.	Тема 8 Управление деятельностью службы безопасности банка	8	4	4				x		4	6	x	ПК-4, ПК-6
5.	Контактная работа	8	38	38				x				4	x
6.	Самостоятельная работа	8						x		40	60		x
7.	Объем дисциплины в семестре	8	38	38				x		40	60	4	x
8.	Всего по дисциплине	x	38	38				x		40	60	4	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Основные положения концепции безопасности банка	2
Л-2	Система угроз безопасности банка. Банк как субъект борьбы с противоправными посягательствами	2
Л-3	Система правового обеспечения безопасности банка. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания	2
Л-4	Банковское законодательство. Нормативные акты Банка России. Внутренние нормативные акты банков	2
Л-5	Организация системы безопасности банка. Субъекты обеспечения безопасности банка. Средства и методы обеспечения безопасности банка	2
Л-6	Организация внутреннего контроля банка. Организация службы безопасности банка. Криминалистическое обеспечение безопасности банковских операций	2
Л-7	Система технических средств обеспечения безопасности банка. Технические средства охраны. Технические средства защиты банковских операций и продуктов	2
Л-8	Технико-криминалистические средства. Использование технико-криминалистических средств и справочных материалов в процессе проведения «внутренней экспертизы»	2
Л-9	Хищения денежных средств при совершении кредитных операций. Мошенничество в сфере потребительского кредитования. Мошенничество в сфере кредитования юридических лиц. Меры обеспечения безопасности кредитных операций	2
Л-10	Хищения денежных средств банка в сфере расчетно-кассового обслуживания. Правовая характеристика преступлений в сфере расчетно-кассового обслуживания. Хищения денежных средств в сфере расчетно-кассового обслуживания юридических лиц. Особенности хищения денежных средств с использованием аккредитивов. Особенности хищения денежных средств с использованием платежных поручений. Хищения денежных средств с использованием чеков. Основные способы хищения денежных средств с использованием систем удаленного	2

	управления счетом («Банк-Клиент» и «Интернет-банкинг»). Хищения денежных средств в сфере расчетно-кассового обслуживания физических лиц. Основные способы хищения денежных средств в сфере обслуживания держателей банковских карт. Основные способы хищения денежных средств из хранилищ банка его персоналом	
Л-11	Правовая характеристика векселя. Риски в сфере вексельного обращения. Преступления против собственности, в которых вексель является предметом посягательства	2
Л-12	Преступления против собственности, в которых вексель является средством совершения преступления. Меры предупреждения преступлений в сфере вексельного обращения	2
Л-13	Злоупотребление полномочиями. Коммерческий подкуп	2
Л-14	Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и иную тайну. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка	2
Л-15	Общие принципы обеспечения безопасности в автоматизированных банковских системах	2
Л-16	Организация и функционирование системы безопасности банка	2
Л-17	Управление деятельностью службы безопасности банка	2
Л-18	Управление деятельностью службы безопасности банка	2
Л-19	Управление деятельностью службы безопасности банка	2
Итого по дисциплине		38

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лабораторных работ	Объем, академические часы
ЛР-1	Основные положения концепции безопасности банка	2
ЛР -2	Основные положения концепции безопасности банка	2
ЛР -3	Основные положения концепции безопасности банка	2
ЛР -4	Основные положения концепции безопасности банка	2
ЛР -5	Классификация угроз. Матрица угроз	2
ЛР -6	Классификация угроз. Матрица угроз	2
ЛР -7	Классификация угроз. Матрица угроз	2

ЛР -8	Классификация угроз. Матрица угроз	2
ЛР -9	Мошенничество. Виды мошенничества	2
ЛР-10	Общие принципы обеспечения безопасности в автоматизированных банковских системах	2
ЛР -11	Общие принципы обеспечения безопасности в автоматизированных банковских системах	2
ЛР -12	Общие принципы обеспечения безопасности в автоматизированных банковских системах	2
ЛР -13	Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	2
ЛР -14	Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	2
ЛР -15	Организация и функционирование системы безопасности банка.	2
ЛР -16	Организация и функционирование системы безопасности банка.	2
ЛР -17	Управление деятельностью службы безопасности банка	2
ЛР -18	Управление деятельностью службы безопасности банка	2
ЛР -19	Управление деятельностью службы безопасности банка	2
Итого по дисциплине		38

5.2.3 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Основные положения концепции безопасности банка	Понятие, содержание и сущность безопасности. Контекст концепции безопасности банка. Объекты безопасности банковских систем	6
2.	Политика безопасности	Политика безопасности. Понятие и модели политики безопасности. Механизмы защиты. Принципы реализации политики безопасности. Оценка безопасности банковских систем.	4
3.	Классификация угроз. Матрица угроз	Характеристика возможных сценариев преступных действий. Злоумышленники. Концептуальная модель	6

			злоумышленника. Характеристика воздействий злоумышленника.	
4.	Мошенничество. мошенничества	Виды	Концептуальная модель мошенничества. Промышленный шпионаж. Концептуальная модель промышленного шпионажа. Теневая экономика и недобросовестная конкуренция. Информация как объект банковской безопасности.	4
5.	Общие принципы обеспечения безопасности автоматизированных банковских системах	в	Принципы информатизации деятельности банка. Требования, предъявляемые к банковским информационным системам. Подходы к обеспечению безопасности банковских систем. Методы и средства организации защиты банковской безопасности.	4
6.	Особенности обеспечения информационной безопасности в автоматизированных банковских системах	в различных	Безопасность в автоматизированных платежных системах. Безопасность в автоматизированных информационных системах. Безопасность в телекоммуникационных системах и системах связи.	6
7.	Организация функционирование безопасности банка	и системы	Организация системы банковской безопасности, структура и функции службы безопасности. Координация и взаимодействие службы безопасности банка с правоохранительными органами. Функции системы банковской безопасности. Обеспечение режима и охраны. Охранная деятельность. Защита системы кадрового обеспечения.	6
8.	Управление	деятельностью	Защита системы кадрового	4

	службы безопасности банка	обеспечения от преступных посягательств. Действия в целях обеспечения личной охраны руководства и персонала банка. Криминалистическое обеспечение банковской безопасности. Теоретические основы криминалистического обеспечения банковской деятельности. Криминалистическая модель банка как объекта преступных посягательств	
Итого по дисциплине			40

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1 Базы данных / Швецов В.И. – М. [электронный ресурс]: Национальный открытый университет “ИНТУИТ” , 2009. – 240 с..

2 Соловьев В.П., Гуренко В.В., Пуцко Н.Н. Безопасность систем баз данных: Учебное пособие для студентов. Под редакцией Соловьева В.П. – М. [электронный ресурс]: МИИТ, 2007. – 90с. .

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Лапони́на, О.Р. Межсетевое экранирование Основы информационной безопасности [электронный ресурс]: Учебное пособие. Издательство: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007 - 344 с.

6.3 Методические указания для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:

- конспект лекций;
- методические указания по выполнению лабораторных работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие, включающее:

- методические рекомендации по самостоятельному изучению вопросов;
- методические рекомендации по подготовке к занятиям.

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Open Office
2. JoliTest (JTRun, JTEditor, TestRun)

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://fstec.ru/normotvorcheskaya/akty>
2. <http://ivo.garant.ru/#/startpage:0>
3. <http://www.consultant.ru/>

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение практических занятий

Номер ЛР	Тема практических занятий	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ЛР-1	Основные положения концепции безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-2	Основные положения концепции безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-3	Основные положения концепции безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel

				4. Microsoft Power Point 5. Paint
ЛР-4	Основные положения концепции безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-5	Классификация угроз. Матрица угроз	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-6	Классификация угроз. Матрица угроз	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-7	Классификация угроз. Матрица угроз	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-8	Классификация угроз. Матрица угроз	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-9	Мошенничество. Виды мошенничества	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint

ЛР-10	Общие принципы обеспечения безопасности в автоматизированных банковских системах	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	<ol style="list-style-type: none"> 1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-11	Общие принципы обеспечения безопасности в автоматизированных банковских системах	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	<ol style="list-style-type: none"> 1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-12	Общие принципы обеспечения безопасности в автоматизированных банковских системах	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	<ol style="list-style-type: none"> 1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-13	Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	<ol style="list-style-type: none"> 1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-14	Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	<ol style="list-style-type: none"> 1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-15	Организация и функционирование системы безопасности банка.	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	<ol style="list-style-type: none"> 1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint

ЛР-16	Организация и функционирование системы безопасности банка.	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-17	Управление деятельностью службы безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-18	Управление деятельностью службы безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ЛР-19	Управление деятельностью службы безопасности банка	948 аудитория - лаборатория технических средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ № 1509 от 01.12.2016

Разработал(и): Набокина О.Я.

Набокина О.Я.