Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»
Кафедра «Информационная безопасность»

ОДОБРЕНО

Методической комиссией по укрупненной группе специальностей и направлений 10.00.00 «Информационная безопасность»
Председатель МК:

Мелехин В.Б.
Подпись ФИО

«17» 10 2018 г.

УТВЕРЖДАЮ:

Декан, председатель совета факультета КТВТиЭ,

Юсуфов Ш.А.
Подпись ФИО

«13» 10 2018г.

Фонд оценочных средств

по дисциплине **«Обеспечение информационной безопасности в банковских системах»** для контроля знаний обучающихся подготовки специалистов 10.05.03. - Информационная безопасность автоматизированных систем, программа специализации Безопасность открытых информационных систем

Составитель Качаева Г.И.

Фонд оценочных средств обсужден на заседании кафедры «Информационная безопасность» «15» 10 2018г., протокол № 2

Зав. кафедрой Качаева Г.И.

Фонд оценочных средств является приложением к рабочей программе по дисциплине С1.В.ДВ.3 «Обеспечение информационной безопасности в интеллектуальных системах»

Махачкала, 2018г.

Оглавление

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ООП

1.1. Перечень компетенций и планируемые результаты

Табл.1

№	Содержание и код компетенций по ФГОС	В результате изучения дисциплины «Обеспечение информационной безопасности в интеллектуальных системах» обучающиеся должны:		
		знать	уметь	владеть
1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1)	основные методы адаптации ИС на основе интеллектуальных методов	реализовывать основные методы адаптации ИС на основе интеллектуальных методов	навыками ведения БД, которые обеспечивают приемлемый уровень интеллектуальной обработки информации
2	способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2)	основные методы настройки информационных систем на основе интеллектуальных методов	использовать основные методы настройки информационных систем на основе интеллектуальных методов	работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
3	способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3)	основы организационного и технического обеспечения мер и средств защиты информации в АБС, используемых в БС РФ	выявлять угрозы и определять их актуальность для современных компьютерных анализировать уровень информационной безопасности АБС, в соответствии с требованиями стандартов, нормативных актов, методических документов в области обеспечения ИБ БС РФ	профессиональной терминологией в области ИБ БС РФ; – навыками работы с технической документацией по обеспечению информационной безопасности БС РФ
4	способностью участвовать в организации и	особенности технологии защиты информации и обеспечения ИБ БС	контролировать уровень выполнения требований защиты	знаниями по оперативному управлению деятельностью

	проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4)	РФ;	информации в банковской организации БС РФ	служб защиты информации в организации БС РФ
5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5)	организацию работы и нормативные документы в области обеспечения защиты информации и сертификации средств и систем защиты информации, используемых в БС РФ	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях БС РФ	методами формирования требований по защите информации в рамках нормативной базы ИБ БС РФ

1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Обеспечение информационной безопасности в интеллектуальных системах» определяется на следующих трех этапах:

1. Этап текущих аттестаций (вх.контр., текущие аттестации 1-3; СРС)
2. Этап промежуточных аттестаций (экзамен)

Таблица 2

Код компетенций по ФГОС	Этапы формирования компетенций по дисциплине «Обеспечение информационной безопасности в интеллектуальных системах»									
	СЕМЕСТРЫ									
	I	II	III-VIII	IX						X
	-	-	-	Этап текущих аттестаций					Этап промеж.аттест.	-
	-	-	-	1 нед.	2-5нед.	6-10 нед.	11-15нед.	1-17 нед.	18-20нед.	-
	-	-	-	Входной контроль	Текущая аттест.1 (контр.раб. 1)	Текущая аттест.2 (контр.раб.2)	Текущая аттест.3 (контр.раб.3)	СРС	Промеж.аттест.	-
1	2	3	4	5	6	7	8	9	11	12
ПСК-4.1	-	-	-	+	+	+	+	+	+	+
ПСК-4.2	-	-	-	+	+	+	+	+	+	+
ПСК-4.3	-	-	-	+	+	+	+	+	+	+
ПСК-4.4	-	-	-	+	+	+	+	+	+	+
ПСК-4.5	-	-	-	+	+	+	+	+	+	+

СРС – самостоятельная работа студентов; КР– курсовая работа; Знак «+» соответствует формированию компетенции.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.

В рамках текущих аттестаций (таблица 2) оценка уровня сформированности компетенций проводится на занятиях:

- лекционного типа посредством экспресс-опроса обучаемых, в том числе по темам и разделам, вынесенных для самостоятельного изучения;
- лабораторного типа путем устного опроса выполненных лабораторных заданий;
- практического типа методами проведения письменных контрольных работ.

Оценка сформированности компетенций в рамках промежуточной аттестации проводится по билетам для зачета. Они включают в себя вопросы для оценки знаний, умений и навыков, т.е. задания:

- *репродуктивного уровня,* позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умения правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;
- *реконструктивного уровня,* позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;
- *творческого уровня,* позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

В ходе проведения текущей и промежуточной аттестации оцениваются:

- полнота и содержательность ответа;
- умение привести примеры из области операционных систем;
- умение пользоваться дополнительной литературой и современными технологиями обучения при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций, учебной литературы, интернет- ресурсам и другим источникам информации.

В ходе проведения оценки сформированности компетенций рекомендуются применение современных компьютерных технологий и виртуальных форм опроса в интерактивном режиме.

2.1. Описание показателей оценивания компетенций

Таблица 3

Оценка «неудовлетворительно» (не зачтено) или отсутствие сформированности компетенции	Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины. Уровень освоения дисциплины, при котором у обучаемого не сформировано	Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне. При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность доформирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования	Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке. Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных	Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи. Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90%

более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции.	компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно».	компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо».	сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций.

2.2. Описание критериев определения уровня сформированности компетенций

Таблица 4

Уровни сформированност	Критерии определения уровня сформированности	Компесенции, формируемые в результате освоения дисциплины ООП				
		Профессиональные компетенции (ПК)				
		ПСК-4.1	ПСК-4.2	ПСК-4.3	ПСК-4.4	ПСК-4.5
Пороговый уровень	Компетенция сформирована	+	+	+	+	+
	Демонстрируется недостаточный уровень самостоятельности навыка					
	Обладает качеством **репродукции**					
Достаточный уровень	Компетенция сформирована	+	+	+	+	+
	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка					
	Обладает качеством **реконструкции**					
Высокий уровень	Компетенция сформирована	+	+	+	+	+
	Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка					
	Обладает **творческим** качеством					

2.3. Описание шкал оценивания

В Дагестанском государственном техническом университете внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Таблица 5

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 -17 баллов	«Хорошо» - 70-84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12-14 баллов	«Удовлетворительно» - 56-69баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – невладения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

2.4. Определение уровня сформированности компетенций в результате изучения дисциплины «Обеспечение информационной безопасности в интеллектуальных системах»

Таблица 6

№	Код компетенций по ФГОС	Уровни сформированности компетенций		
		Пороговый	Достаточный	Высокий
1	2	3	4	5
1	ПСК-4.1	**Знает** основные методы адаптации ИС на основе интеллектуальных методов **(на пороговом уровне, или на « удовлетворительно»).** **Умеет** реализовывать основные методы адаптации ИС на основе интеллектуальных методов **слабо.** **Владеет** навыками ведения БД, которые обеспечивают приемлемый уровень интеллектуальной обработки информации **слабо.**	**Знает** основные методы адаптации ИС на основе интеллектуальных методов **на достаточном уровне («на «хорошо»).** **Умеет** реализовывать основные методы адаптации ИС на основе интеллектуальных методов **на достаточном уровне.** **Владеет** навыками ведения БД, которые обеспечивают приемлемый уровень интеллектуальной обработки информации **на достаточном уровне.**	**Знает** основные методы адаптации ИС на основе интеллектуальных методов **полноценно (на высоком уровне, на «отлично»).** **Умеет** реализовывать основные методы адаптации ИС на основе интеллектуальных методов **полноценно.** **Владеет** навыками ведения БД, которые обеспечивают приемлемый уровень интеллектуальной обработки информации **полноценно.**
2	ПСК-4.2	**Знает** основные методы настройки информационных систем на основе интеллектуальных методов **(на пороговом уровне, или на « удовлетворительно»).** **Умеет** использовать основные методы настройки информационных систем на основе интеллектуальных методов **слабо.**	**Знает** основные методы настройки информационных систем на основе интеллектуальных методов **на достаточном уровне («на «хорошо»).** **Умеет** использовать основные методы настройки информационных систем на основе интеллектуальных методов **на достаточном уровне.** **Владеет**	**Знает** основные методы настройки информационных систем на основе интеллектуальных методов **полноценно (на высоком уровне, на «отлично»).** **Умеет** использовать основные методы настройки информационных систем на основе интеллектуальных методов **полноценно.** **Владеет** работы по установке, настройке и

		Владеет работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации **слабо.**	работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации **на достаточном уровне.**	обслуживанию программных, программно-аппаратных и технических средств защиты информации **полноценно.**
3	ПСК-4.3	**Знает** основы организационного и технического обеспечения мер и средств защиты информации в АБС, используемых в БС РФ **(на пороговом уровне, или на « удовлетворительно»).** **Умеет** выявлять угрозы и определять их актуальность для современных компьютерных анализировать уровень информационной безопасности АБС, в соответствии с требованиями стандартов, нормативных актов, методических документов в области обеспечения ИБ БС РФ **слабо.** **Владеет** профессиональной терминологией в области ИБ БС РФ; – навыками работы с технической документацией по обеспечению информационной безопасности БС РФ **слабо.**	**Знает** основы организационного и технического обеспечения мер и средств защиты информации в АБС, используемых в БС РФ **на достаточном уровне («на «хорошо»).** **Умеет** выявлять угрозы и определять их актуальность для современных компьютерных анализировать уровень информационной безопасности АБС, в соответствии с требованиями стандартов, нормативных актов, методических документов в области обеспечения ИБ БС РФ **на достаточном уровне.** **Владеет** профессиональной терминологией в области ИБ БС РФ; – навыками работы с технической документацией по обеспечению информационной безопасности БС РФ **на достаточном уровне.**	**Знает** основы организационного и технического обеспечения мер и средств защиты информации в АБС, используемых в БС РФ **полноценно (на высоком уровне, на «отлично»).** **Умеет** выявлять угрозы и определять их актуальность для современных компьютерных анализировать уровень информационной безопасности АБС, в соответствии с требованиями стандартов, нормативных актов, методических документов в области обеспечения ИБ БС РФ **полноценно.** **Владеет** профессиональной терминологией в области ИБ БС РФ; – навыками работы с технической документацией по обеспечению информационной безопасности БС РФ **полноценно.**
4	ПСК-4.4	**Знает** особенности технологии защиты информации и обеспечения ИБ БС РФ	**Знает** особенности технологии защиты информации и обеспечения ИБ БС РФ	**Знает** особенности технологии защиты информации и обеспечения ИБ БС РФ

		(на пороговом уровне, или на « удовлетворительно»). **Умеет** контролировать уровень выполнения требований защиты информации в банковской организации БС РФ **слабо.** **Владеет** знаниями по оперативному управлению деятельностью служб защиты информации в организации БС РФ **слабо.**	**на достаточном уровне («на «хорошо»).** **Умеет** контролировать уровень выполнения требований защиты информации в банковской организации БС РФ **на достаточном уровне.** **Владеет** знаниями по оперативному управлению деятельностью служб защиты информации в организации БС РФ **на достаточном уровне.**	**полноценно (на высоком уровне, на «отлично»).** **Умеет** контролировать уровень выполнения требований защиты информации в банковской организации БС РФ **полноценно.** **Владеет** знаниями по оперативному управлению деятельностью служб защиты информации в организации БС РФ **полноценно.**
5	ПСК-4.5	**Знает** организацию работы и нормативные документы в области обеспечения защиты информации и сертификации средств и систем защиты информации, используемых в БС РФ **(на пороговом уровне, или на « удовлетворительно»).** **Умеет** разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях БС РФ **слабо.** **Владеет** методами формирования требований по защите информации в рамках нормативной базы ИБ БС РФ **слабо.**	**Знает** организацию работы и нормативные документы в области обеспечения защиты информации и сертификации средств и систем защиты информации, используемых в БС РФ **на достаточном уровне («на «хорошо»).** **Умеет** разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях БС РФ **на достаточном уровне.** **Владеет** методами формирования требований по защите информации в рамках нормативной базы ИБ БС РФ **на достаточном уровне.**	**Знает** организацию работы и нормативные документы в области обеспечения защиты информации и сертификации средств и систем защиты информации, используемых в БС РФ **полноценно (на высоком уровне, на «отлично»).** **Умеет** разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях БС РФ **полноценно.** **Владеет** методами формирования требований по защите информации в рамках нормативной базы ИБ БС РФ **полноценно.**

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения ООП.

3.1. Задания для входного контроля

1.Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).

3.2 Вопросы для текущих контрольных работ

3.2.1 Аттестационная контрольная работа №1

1. Предмет и задачи дисциплины «Защита информации в банковских системах».
2. Нормативно – правовые документы, регламентирующие вопросы защиты информации и информационной безопасности.
3. Банк России как регулятор деятельности коммерческих банков. Нормативная база обеспечения деятельности банков в вопросах защиты информации и информационной безопасности.
4. Операционный риск в деятельности кредитных организаций. Порядок управления и оценки указанным видом риска.
5. Виды информации, возможные ограничения ее использования и распространения.
6. Перечень сведений, который может быть отнесен к банковской тайне, порядок их представления сторонним лицам.
7. Информация, ее роль в современном мире, носители информации и их виды. Порядок защиты носителей информации, его отличия от мероприятий по защите информации.
8. Требования к кредитным организациям при осуществлении переводов денежных средств (Положение ЦБ РФ № 382-П).
9. Информация как нематериальные активы компании, показатели оценки информации как соответствующих ресурсов.

3.2.2 Аттестационная контрольная работа №2

1. Финансовая информация (понятие, цели получения, виды классификации).
2. История развития (поколения) АБС в банковской системе РФ, общие характеристики автоматизированных банковских систем, используемых в кредитных организациях.
3. Элементы и программно - функциональные модули АБС, виды информационных банковских технологий, используемых при создании АБС.
4. Уязвимости АБС, архитектура систем защиты и способы защиты от неправомерных действий.
5. Платежная система РФ, цели и основные элементы, участники, нормативно – правовая база регламентирующие соответствующие вопросы.
6. 13. Платежная система Банка России - история развития, основные задачи, отдельные
7. элементы и системы расчетов, входящие в ее состав.
8. Система банковских электронных срочных платежей (БЭСП) Банка России – порядок, условия и принципы функционирования, требования к участникам.

9. Региональная автоматизированная банковская информационная система (РАБИС – НП) - назначение, принципы построения, участники расчетов и пользователи, распределение функций.

3.3.3 Аттестационная контрольная работа №3

Тестовые задания

1. Какая информация в соответствии с действующим законодательством может быть отнесена к категории общедоступной:
а. информация о нормативно – правовых актах, затрагивающая права, свободы и обязанности граждан;
б. информация об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
в. информация о государственных золотовалютных резервах РФ;
г. все виды информации, указанные в п.п. а-в
2. В соответствии с нормативными актами регулятора – Банка России к какому виду относятся риски банков, связанные с осуществлением контроля информационных потоков и обеспечением информационной безопасности:
а. рыночный риск;
б. правовой риск;
в. операционный риск;
г. кредитный риск;
д. риск потери деловой репутации.
3. Какие виды банков вправе осуществлять свою деятельность на территории РФ в соответствии с действующим законодательством:
а. универсальные банки;
б. инвестиционные банки;
в. региональные банки;
г. ссудно-сберегательные кассы;
д. банки, указанные в п.п. а-в.
4. Какие из указанных целей стандартизации деятельности по обеспечению ИБ кредитных организаций РФ относятся к категории основных:
а. развитие и укрепление банковской системы РФ, повышение доверия к ней;
б. достижение адекватности мер защиты реальным угрозам ИБ;
в. предотвращение и (или) снижение ущерба от инцидентов ИБ;
г. цели, указанные в п.п. а-б;
д. цели, указанные в п.п. а-в.
5. Представителям каких государственных органов могут выдаваться справки по счетам юридических лиц и предпринимателей без образования юридического лица:
а. судам общей юрисдикции и арбитражным судам;
б. налоговым и таможенным органам;
в. органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений;
г. субъектам, указанных в п.п. а-б;
д. субъектам, указанным в п.п. а-в.
6. Какая из указанной информации не подлежит обязательному раскрытию банками неограниченному кругу пользователей в соответствии с действующими нормативными актами банка России:
а. информация о составе органов управления кредитной организации;
б. информация о решениях принятых исполнительными органами кредитной организации;
в. годовая бухгалтерская (финансовая) отчетность банка;
г. расчет собственных средств (капитала) банка;
д. информация, указанная в п.п. в-г.
7. Информация может оцениваться как следующий вид активов компании:

а. внеоборотные активы;
б. нематериальные активы;
в. оборотные активы;
г. товарно -материальные ценности;
8. К основным характеристикам финансовой информации могут быть отнесены следующие:
а.уместность;
б. надежность;
в. важность;
г. характеристики, указанные в п.п. а-б;
д. характеристики, указанные в п.п. а-в.
9. Единое информационное пространство банка основывается на следующих принципах:
а. открытости;
б. ограничения количества пользователей;
в. защищенности;
г. на принципах, указанных в п.а и п.в;
д. на принципах, указанных в п.п.а-в.
10. Автоматизированные банковские системы могут быть построены на основе следующих технологий:
а. платежных;
б. операционных;
в. документарных;
г. технологий, указанных в п.п. а-в;
д. технологий, указанных в п.п. б-в.
11. К настоящему времени экспертами выделяются следующее количество поколений российских автоматизированных банковских систем (АБС):
а. четыре;
б. пять;
в. шесть;
д. семь.
12. Какие функциональные модули, как правило, включаются в состав АБС коммерческих банков:
а. модуль расчетно-кассового обслуживания клиентов;
б. модуль кредитных операций клиентов;
в. модуль хозяйственных договоров и обеспечения внутрибанковской деятельности;
г. функциональные модули, указанные в п. а-б;
д. функциональные модули, указанные в п. а-в.
13. Какие информационные угрозы могут быть характерны доступным компонентам АБС:
а. несанкционированный доступ к ресурсам и данным системы
б. подмена сетевых адресов;
в. отказ в обслуживании;
г. атака на уровне приложений;
д. все информационные угрозы, указанные в п.п. а- г.
14. Что из указанного не относится к возможным причинам появления уязвимостей АБС: а. отсутствие гарантий конфиденциальности и целостности передаваемых данных;
б. утеря актуальности разработанной политики ИБ или некорректная (неполная) ее реализация;
в. отсутствие или недостаточный уровень защиты от несанкционированного доступа (антивирусы, организация и функционирование системы контроля доступа, систем обнаружения атак);
г. низкий (непрофессиональный) уровень администрирования АБС и сетевых приложений;
д. относятся все причины, указанные в п.п. а-г.
15. Платежная система Банка России является:
а. централизованной;

б. децентрализованной;
в. распределенной.
16. Какая из систем расчетов (элементов) не входит в состав платежной системы Банка России:
а. система внутрирегиональных электронных расчетов (система ВЭР);
б. система межрегиональных электронных расчетов (система МЭР);
в. система международных электронных расчетов (система МДЭР);
г. система банковских электронных срочных платежей (система БЭСП);
д. входят все системы расчетов, указанные в п.п. а-г.
17. Какие из указанных источников угроз информационной безопасности (ИБ) Банка не относятся к категории основных:
а. работники банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий;
б. работники банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками банка, но осуществляющие попытки
несанкционированного доступа в АБС;
в. криминальные элементы и террористы;
г. неблагоприятные события природного, техногенного и социального характера;
д. к основным, относятся все категории угроз, указанные в п.п. а-г..
18. Политика ИБ банка формируется на основе следующих элементов:
а. требований законодательства РФ и нормативных актов ЦБ РФ;
б. интересов и бизнес – целей банка;
в. накопленного в организации опыта в области обеспечения ИБ;
г. на основе элементов, указанных в п.а и п.в;
д. на основе элементов, указанных в п.п. а-в.
19. Какой из указанных органов корпоративного управления банка может иметь полномочия по утверждению Политики информационной безопасности данной кредитной организации:
а. Наблюдательный Совет;
б. Правление;
г. Председатель Правления;
д. любой из указанных органов управления.
20. Какой из указанных документов, входящих в пакет стандарта СТО БР ИББС (5-актуальная версия) имеет рекомендательный характер для использования кредитными организациями:
а. БР ИББС-1.0-2014. «Общие положения» (5 редакция);
б. БР ИББС-1.1-2017. «Аудит информационной безопасности» СТО БР ИББС-1.0-2014. «Общие положения» (5 редакция);
в. БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности»;
г. БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы РФ требованиям СТО БР ИББС-1.0-2014 (4 редакция).
21. В соответствии с нормативными документами Банка России оператор по переводу денежных средств – банк обеспечивает реализацию запрета выполнения одним лицом в один момент времени следующих ролей:
а. ролей, связанных с проектированием (разработкой) и созданием (модернизацией) объекта информационной инфраструктуры;
б. ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и в части его технического обслуживания или ремонта;
в. Ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и его эксплуатации;
г. ролей, указанных в п.а и п.б;
д. ролей, указанных в п.б и п.в.

22. В соответствии с требованиями нормативных документов ЦБ РФ служба информационной безопасности банка при осуществлении переводов денежных средств должна быть наделена следующими полномочиями:
а. осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации;
б. определять требования к техническим средствам защиты информации и организационным мерам защиты информации;
в. определять порядок эксплуатации технических средств защиты информации и соответствующего программного обеспечения;
г. полномочиями, указанными в п.п. а-б;
д. полномочиями, указанными в п.п. а-в.

3.3 Перечень вопросов на зачет

1. Предмет и задачи дисциплины «Защита информации в банковских системах».
2. Нормативно – правовые документы, регламентирующие вопросы защиты информации и информационной безопасности.
3. Банк России как регулятор деятельности коммерческих банков. Нормативная база обеспечения деятельности банков в вопросах защиты информации и информационной безопасности.
4. Операционный риск в деятельности кредитных организаций. Порядок управления и оценки указанным видом риска.
5. Виды информации, возможные ограничения ее использования и распространения.
6. Перечень сведений, который может быть отнесен к банковской тайне, порядок их представления сторонним лицам.
7. Информация, ее роль в современном мире, носители информации и их виды. Порядок защиты носителей информации, его отличия от мероприятий по защите информации.
8. Требования к кредитным организациям при осуществлении переводов денежных средств (Положение ЦБ РФ № 382-П).
9. Информация как нематериальные активы компании, показатели оценки информации как соответствующих ресурсов.
10. Финансовая информация (понятие, цели получения, виды классификации).
11. История развития (поколения) АБС в банковской системе РФ, общие характеристики автоматизированных банковских систем, используемых в кредитных организациях.
12. Элементы и программно - функциональные модули АБС, виды информационных банковских технологий, используемых при создании АБС.
13. Уязвимости АБС, архитектура систем защиты и способы защиты от неправомерных действий.
14. Платежная система РФ, цели и основные элементы, участники, нормативно – правовая база регламентирующие соответствующие вопросы.
15. 13. Платежная система Банка России - история развития, основные задачи, отдельные
16. элементы и системы расчетов, входящие в ее состав.
17. Система банковских электронных срочных платежей (БЭСП) Банка России – порядок, условия и принципы функционирования, требования к участникам.
18. Региональная автоматизированная банковская информационная система (РАБИС – НП) - назначение, принципы построения, участники расчетов и пользователи, распределение функций.
19. Отраслевые стандарты по информационной безопасности Банка России СТО БР ИББС.
20. Основные положения, разделы и элементы, история развития.

21. Формирование перечня конфиденциальных сведений и информации банка, модели угроз и нарушителей информационной безопасности.
22. Определение потенциальных каналов утечки (перехвата) конфиденциальной информации банка, перечня и состава прикладных методов защиты информации.
1. Ответственность, полномочия и права службы информационной безопасности банка, ее сотрудников и руководителя.
23. Организация системы обеспечения информационной безопасности банка (система информационной безопасности, система менеджмента информационной безопасности).
24. Обработка кредитными организациями информации, содержащей персональные данные.
25. Обеспечение информационной безопасности соответствующих банковских технологических процессов.
26. Аудит информационной безопасности кредитных организаций (концепция, основные принципы, менеджмент программы, последовательность и этапы проведения).
27. Организация системы информационной безопасности для защиты информации при осуществлении кредитными организациями дистанционного банковского обслуживания (ДБО) своих клиентов.
28. Применение средств защиты (антивирусных программ) от вредоносного кода (ВК) в целях защиты информации при осуществлении банковской деятельности.

3.4 Вопросы для проверки остаточных знаний по дисциплине «Обеспечение информационной безопасности в интеллектуальных системах»

29. Основные положения, разделы и элементы, история развития.
30. Формирование перечня конфиденциальных сведений и информации банка, модели угроз и нарушителей информационной безопасности.
31. Определение потенциальных каналов утечки (перехвата) конфиденциальной информации банка, перечня и состава прикладных методов защиты информации.
2. Ответственность, полномочия и права службы информационной безопасности банка, ее сотрудников и руководителя.
32. Организация системы обеспечения информационной безопасности банка (система информационной безопасности, система менеджмента информационной безопасности).
33. Обработка кредитными организациями информации, содержащей персональные данные.
34. Обеспечение информационной безопасности соответствующих банковских технологических процессов.
35. Аудит информационной безопасности кредитных организаций (концепция, основные принципы, менеджмент программы, последовательность и этапы проведения).
36. Организация системы информационной безопасности для защиты информации при осуществлении кредитными организациями дистанционного банковского обслуживания (ДБО) своих клиентов.

1. Применение средств защиты (антивирусных программ) от вредоносного кода (ВК) в целях защиты информации при осуществлении банковской деятельности

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

В качестве методического материала рекомендуется использовать:

1. Положение о ФОС в ФГБОУ ВО «Дагестанский государственный технический университет» (Приложение № 9 к ООП).

2. Положение ФГБОУ ВО «Дагестанский государственный технический университет» о модульно-рейтинговой системе оценки учебной деятельности студентов.
3. Процедура проведения оценочных мероприятий.

4.1. Процедура проведения оценочных мероприятий

4.1.1. Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля (текущей аттестации) можно отнести устный опрос, письменные задания, контрольные работы.

Основные этапы текущего контроля:

– в конце каждой лекции или лабораторного занятия студентам выдаются задания для внеаудиторного выполнения по соответствующей теме;

– срок выполнения задания устанавливается по расписанию занятий (к очередной лекции или лабораторному занятию);

– студентам, пропускающим занятия, выдаются дополнительные задания – представить конспект пропущенного занятия, написанный «от руки» с последующим собеседованием по теме занятия;

– подведение итогов контроля проводится по графику проведения текущего контроля;

– результаты оценки успеваемости заносятся в рейтинговую ведомость и доводятся до сведения студентов;

К достоинствам данного типа относится его систематичность, непосредственно коррелирующаяся с требованием постоянного и непрерывного мониторинга качества обучения, а также возможность бально-рейтинговой оценки успеваемости обучающихся.

Недостатком является фрагментарность и локальность проверки. Компетенцию целиком, а не отдельные ее элементы (знания, умения, навыки) при подобном контроле проверить невозможно.

4.1.2.Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов).

Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Достоинства: помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций.

Форма промежуточной аттестации: **зачет**.

Текущий контроль и промежуточная аттестация традиционно служат основным средством обеспечения в учебном процессе «обратной связи» между преподавателем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики преподавания учебных дисциплин.

Основные этапы промежуточной аттестации:

- зачет проводится по расписанию сессии;
- форма проведения занятия – письменная контрольная работа;
- вид контроля – фронтальный;
- требование к содержанию контрольной работы – дать краткий ответ на поставленный вопрос (задание);
- количество вопросов в билете;
- итоговая оценка определяется как сумма оценок, полученных в текущей аттестации и по результатам написания контрольной работы;
- проверка ответов и объявление результатов производится в день написания контрольной работы;
- результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента (при получении зачета).

Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

При первой попытке ликвидации задолженности, во время зачетной недели или в течение сессии, студенту выдаются все задания по текущему контролю и промежуточной аттестации, по которым он не смог набрать зачетное количество баллов.