Приложение А

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Обеспечение ИБ в банковской системе»

Уровень образования **специалитет**
(бакалавриат/магистратура/специалитет)

Специальность **10.05.03 Информационная безопасность автоматизированных систем**
(код, наименование специальности)

Специализация **Безопасность открытых информационных систем**
(наименование)

Разработчик _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол № 2

Зав. кафедрой _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Обеспечение ИБ в банковской системе» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Рабочей программой дисциплины «Обеспечение ИБ в банковской системе» предусмотрено формирование следующих компетенций:

ПК-4. Способен осуществлять формирование требований к защите информации в автоматизированных системах.

ПК-4	Способен осуществлять формирование требований к защите информации в автоматизированных системах	ПК-4.З.2. Знать: особенности защиты информации в открытых информационных системах
		ПК-4.У.1. Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
		ПК-4.У.4. Уметь: определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)

- *Устный опрос*
- *Вопросы для проведения экзамена*

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем1
ПК – 4 Способен осуществлять формирование требований к защите информации в автоматизированных системах	ПК-4.З.2. Знать: особенности защиты инф формации в открытых информационных системах	Знать: Основные правила разработки политики безопасности организации. Компоненты политики безопасности; угрозы безопасности и методы защиты информации в банковских инф формационных системах; организацию работы и нормативные документы в области обеспечения защиты информации и сертификации средств и систем защиты информации, используемых в БС РФ; Уметь: выявлять угрозы системе безопасности банка и разрабатывать комплекс мер по ее совершенствованию 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; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях БС РФ; Владеть: методами формирования требований по защите информации в рамках нормативной базы ИБ БС РФ; оценки эффективности систем защиты информации банковских систем; навыки применения комплексного подхода к обеспечению информационной безопасности банковских систем	№№1-17
	ПК-4.У.1. Уметь: классифицировать защищаемую инф формацию по видам тайны и степеням конфиденциальности;		
	ПК-4.У.4. Уметь: определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.		

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Обеспечение ИБ в банковской системе определяется на следующих этапах:

1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2)*

2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
ПК – 4 Способен осуществлять формирование требований к защите информации в автоматизированных системах	ПК-4.З.2. Знать: особенности защиты ин┐ формации в открытых информационных системах	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ПК-4.У.1. Уметь: классифицировать защищаемую ин┐ формацию по видам тайны и степеням конфиденциальности;						
	ПК-4.У.4. Уметь: определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.						

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины Обеспечение ИБ в банковской системе является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 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 – 69 баллов	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; – не владения 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.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

3.1. Задания и вопросы 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. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Предмет дисциплины, история создания и развития банковской системы РФ, автоматизация банковской деятельности.
2. Создание специализированной структур и подразделений кредитных организаций, занимающихся вопросами безопасности и защиты информации в банковской системе РФ.
3. Значение информации и ее защиты, носители информации.
4. Роль информации в современном мире, виды носителей информации.
5. Актуальность защиты информации, промышленный шпионаж.
6. Характеристики информации.
7. Классификация и характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях (БО) РФ (Платёжные и не платёжные).

3.2.2. Аттестационная контрольная работа №2

1. Задачи ИБ в АБС.
2. Единое информационное пространство банка.
3. Классификация и основные характеристики АБС, эксплуатирующихся в ЦБ РФ и банковских организациях.
4. Элементы и модули АБС, информационные технологии используемые для их построения, уязвимости..
5. Организация деятельности по обеспечению информационной безопасности в кредитных организациях.
6. Модели угроз и нарушителей
7. Организация и функционирования системы обеспечения информационной безопасности в коммерческих банках.

3.2.3. Аттестационная контрольная работа №3

1. Модели угроз и нарушителей
2. Организация и функционирования системы обеспечения информационной безопасности в коммерческих банках.
3. Объекты защиты, виды угроз и типы нарушителей, менеджмент системы информационной безопасности.
4. Формирование и развитие системы расчётов Банка России, элементы платежной системы ЦБ РФ, технологии построения.
5. История формирования и развития, модернизации, эксплуатации и модернизации платежной системы Банка России, элементы входящие в ее состав.
6. Региональная автоматизированная банковская информационная система "РАБИС-НП", принципы и порядок функционирования.

7. Характеристика структуры, оценка безопасности и надёжности централизованной платёжной системы РФ, основанной на базе системы - РАБИС-НП.
8. Банковские электронные срочные платежи (БЭСП), требования к кредитным организациям для вхождения и работе в системе БЭСП
9. Управление рисками платежной системы Банка России, обеспечение безопасности и надёжности ее функционирования.
10. Система банковских электронные срочные платежи (БЭСП), требования Банка России к кредитным организациям для участия в системе, организация их деятельности
11. Стандарты Банка России СТО БР ИББС-2014.

3.3 Список вопросов к экзамену

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.

23. Ответственность, полномочия и права службы информационной безопасности банка, ее сотрудников и руководителя.
24. Организация системы обеспечения информационной безопасности банка (система информационной безопасности, система менеджмента информационной безопасности).
25. Обработка кредитными организациями информации, содержащей персональные данные.
26. Обеспечение информационной безопасности соответствующих банковских технологических процессов.
27. Аудит информационной безопасности кредитных организаций (концепция, основные принципы, менеджмент программы, последовательность и этапы проведения).
28. Организация системы информационной безопасности для защиты информации при осуществлении кредитными организациями дистанционного банковского обслуживания (ДБО) своих клиентов.
29. 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»

1. Основные положения, разделы и элементы, история развития.
2. Формирование перечня конфиденциальных сведений и информации банка, модели угроз и нарушителей информационной безопасности.
3. 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.
4. Организация системы обеспечения информационной безопасности банка (система информационной безопасности, система менеджмента информационной безопасности).
5. Обработка кредитными организациями информации, содержащей персональные данные.
6. Обеспечение информационной безопасности соответствующих банковских технологических процессов.
7. Аудит информационной безопасности кредитных организаций (концепция, основные принципы, менеджмент программы, последовательность и этапы проведения).
8. Организация системы информационной безопасности для защиты информации при осуществлении кредитными организациями дистанционного банковского обслуживания (ДБО) своих клиентов.

3.5 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.

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

Форма экзаменационного билета (пример оформления)

Министерство науки и высшего образования РФ

ФГБОУ ВО "Дагестанский государственный технический университет"

Дисциплина (модуль) **Обеспечение ИБ в банковской системе**
Код, специальность 10.05.03 Информационная безопасность автоматизированных систем .....
Специализация Безопасность открытых информационных систем
Кафедра ИБ Курс 4 Семестр 9
Форма обучения – очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

1. Стандарты Банка России.
2. . Организация и функционирования системы обеспечения информационной безопасности в коммерческих банках.

Экзаменатор.....ФИО.

Утвержден на заседании кафедры (протокол №___ от _____20___ г.)

Зав. кафедрой (название) .....ФИО.

В ФОС размещается пример заполненного экзаменационного билета. Весь комплект экзаменационных билетов по дисциплине хранится на кафедре в соответствии с утвержденной номенклатурой дел.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;
- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка **«отлично»:** обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»:** обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»:** обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»:** обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).