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 «Информационная безопасность открытых систем**»**

Уровень образования — бакалавриат
(бакалавриат/магистратура/специалитет)

Направление подготовки бакалавриата/магистратуры/специальность — **10.03.01 – Информационная безопасность**
(код, наименование направления подготовки/специальности)

Профиль направления подготовки/специализация — Безопасность автоматизированных систем
(наименование)

Разработчик _____ Качаева Г.И .ст. препод. каф. ИБ
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры _____ «___»_____ 20___г., протокол №_____

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

г. Махачкала 2021

Оглавление

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Информационная безопасность открытых систем» 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 направлению подготовки/специальности 10.03.01 – «Информационная безопасность».

Рабочей программой дисциплины «Информационная безопасность открытых систем» предусмотрено формирование следующих компетенций:

1. *ОПК-5Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;*
2. *ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;*
3. *ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;*
4. *ОПК 4.1. - Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах .*

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.

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 тем
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1. знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации	***Знать:*** основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации	Тема 1. Стандартизация и модельное представление открытых информационных систем.
	ОПК-5.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	***Знать*** правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	
	ОПК-5.3 знает правовые основы организации защиты государственной тайны и конфиденциальной информации	***Знать*** правовые основы организации защиты государственной тайны и конфиденциальной информации	
	ОПК-5.4 знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	***Знать*** правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	
	ОПК-5.5 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	***Уметь*** формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	
	ОПК-5.6 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей	***Уметь*** обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей	
	ОПК-5.7 знает правовые основы организации делопроизводства, виды и состав документации	***Уметь*** правовые основы организации делопроизводства, виды и состав документации современной организации,	

	современной организации, особенности документирования профессиональной деятельности	особенности документирования профессиональной деятельности	
	ОПК-5.8 умеет определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы.	***Уметь*** определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы.	
ОПК-6.Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 знает систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации	***Знать*** систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации	Тема 2. Интранет как открытая система. Тема 3. Уязвимость открытых систем на примере интранета.
	ОПК-6.2 знает систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации	***Знать*** систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации	
	ОПК-6.3 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях	***Знать*** задачи органов защиты государственной тайны и служб защиты информации на предприятиях	
	ОПК-6.4 знает систему правовых и организационных мер, направленных на защиту документальных материалов ограниченного доступа	***Знать*** систему правовых и организационных мер, направленных на защиту документальных материалов ограниченного доступа	
	ОПК-6.5 умеет определить политику контроля доступа работников к информации ограниченного доступа	***Уметь*** определить политику контроля доступа работников к информации ограниченного доступа	
	ОПК-6.6 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	***Уметь*** формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	
ОПК-10. Способен в качестве	ОПК-10.1 знает программно-аппаратные средства защиты информации в типовых операционных системах, системах	***Знать*** программно-аппаратные средства защиты информации в типовых операционных системах, системах управления	Тема 4. Атаки на открытые системы Тема 5. Обеспечение

технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	управления базами данных, компьютерных сетях	базами данных, компьютерных сетях	информационной безопасности в открытых системах. Тема 6. Аутентификация субъектов и объектов взаимодействия в открытых системах.
	ОПК-10.2 умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	***Уметь*** конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	
	ОПК-10.3 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	***Знать*** основные угрозы безопасности информации и модели нарушителя объекта информатизации	
	ОПК-10.4 знает цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью	***Знать*** цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью	
	ОПК-10.5 знает принципы формирования политики информационной безопасности объекта информатизации	***Знать*** принципы формирования политики информационной безопасности объекта информатизации	
	ОПК-10.6 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации	***Уметь*** разрабатывать модели угроз и модели нарушителя объекта информатизации	
	ОПК-10.7 умеет оценивать информационные риски объекта информатизации	***Уметь*** оценивать информационные риски объекта информатизации	
	ОПК-10.8 знает принципы организации информационных систем в соответствии с требованиями по защите информации	***Знать*** принципы организации информационных систем в соответствии с требованиями по защите информации	
	ОПК-10.9 знает особенности комплексного подхода к обеспечению информационной безопасности организации	***Знать*** особенности комплексного подхода к обеспечению информационной безопасности организации	
	ОПК-10.10 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	***Уметь*** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
	ОПК-10.11 умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	***Уметь*** разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	
ОПК 4.1. - Способен проводить организационные	ОПК-4.1.1. Знает задачи программно-технического обеспечения информационной безопасности в организации и политику безопасности в операционных системах.	***Знать*** задачи программно-технического обеспечения информационной безопасности в организации и политику безопасности в операционных системах.	Тема 7. Виртуальные вычислительные сети. Тема 8. Межсетевые экраны.

мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.2. Умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.	***Уметь*** выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.	
	ОПК-4.1.3. Умеет пользоваться основными методами и способами информационной безопасности, ориентироваться в видах вредоносных программ и способах борьбы с ними.	***Уметь*** пользоваться основными методами и способами информационной безопасности, ориентироваться в видах вредоносных программ и способах борьбы с ними.	
	ОПК-4.1.4. Умеет настраивать политику безопасности современных операционных систем, решать задачи распределения ресурсов и прав доступа.	***Уметь*** настраивать политику безопасности современных операционных систем, решать задачи распределения ресурсов и прав доступа.	
	ОПК-4.1.5. Владеет навыками разработки и применения системы безопасности, прикладными и инструментальными средствами создания систем информационной безопасности.	***Владеть*** навыками разработки и применения системы безопасности, прикладными и инструментальными средствами создания систем информационной безопасности.	

2.1.1. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Информационная безопасность открытых систем» 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**
ОПК-5Способен	ОПК-5.1 знает основы законодательства Российской Федерации, систему	Контрольная работа	Контрольная работа	Контрольная работа	реферат		Проведения зачёта / экзамена

применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации	№1	№2	№3			
	ОПК-5.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности						
	ОПК-5.3 знает правовые основы организации защиты государственной тайны и конфиденциальной информации						
	ОПК-5.4 знает правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации						
	ОПК-5.5 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации						
	ОПК-5.6 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей						
	ОПК-5.7 знает правовые основы организации делопроизводства, виды и состав документации современной организации, особенности документирования профессиональной деятельности						
	ОПК-5.8 умеет определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы.						

ОПК-6.Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 знает систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации ОПК-6.2 знает систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации ОПК-6.3 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях ОПК-6.4 знает систему правовых и организационных мер, направленных на защиту документальных материалов ограниченного доступа ОПК-6.5 умеет определить политику контроля доступа работников к информации ограниченного доступа ОПК-6.6 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	реферат		Проведения зачёта / экзамена
ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1. Знает задачи программно-технического обеспечения информационной безопасности в организации и политику безопасности в операционных системах. ОПК-4.1.2. Умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	реферат		Проведения зачёта / экзамена

	ОПК-4.1.3. Умеет пользоваться основными методами и способами информационной безопасности, ориентироваться в видах вредоносных программ и способах борьбы с ними.						
	ОПК-4.1.4. Умеет настраивать политику безопасности современных операционных систем, решать задачи распределения ресурсов и прав доступа.						
	ОПК-4.1.5. Владеет навыками разработки и применения системы безопасности, прикладными и инструментальными средствами создания систем информационной безопасности.						
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1 знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	реферат		Проведения зачёта / экзамена
	ОПК-10.2.1умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности						
	ОПК-10.1.2знает основные угрозы безопасности информации и модели нарушителя объекта информатизации						
	ОПК-10.1.3знает цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью						
	ОПК-10.1.4знает принципы формирования политики информационной безопасности объекта информатизации						
	ОПК-10.2.2умеет разрабатывать модели угроз и модели нарушителя объекта информатизации						
	ОПК-10.2.3умеет оценивать информационные риски объекта информатизации						

	ОПК-10.1.5знает принципы организации информационных систем в соответствии с требованиями по защите информации						
	ОПК-10.1.6 знает особенности комплексного подхода к обеспечению информационной безопасности организации						
	ОПК-10.2.4умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите						

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 «Информационная безопасность открытых систем» 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	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
	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: 1. незнания значительной части программного материала; 2. не владения понятийным аппаратом дисциплины; 3. допущения существенных ошибок при изложении учебного материала; 4. неумение строить ответ в соответствии со структурой излагаемого вопроса; 5. 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. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.
2. Атаки на открытые системы.
3. Анализ угроз ИБ ресурсам интранета и причины их реализации.

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Стандартизация и модельное представление открытых информационных систем.
2. Роль стандартов в технологии открытых систем.
3. Основные группы стандартов и организации по стандартизации.
4. Модель OSI и POSIX. Интранет как открытая система.
5. Разработка и управление Политикой использования ресурсов интранета.
6. Уязвимость открытых систем на примере интранета
7. Анализ угроз ИБ ресурсам интранета и причины их реализации.
8. Уязвимости операционных систем, серверов, рабочих станций, каналов связи.
9. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, WorldWideWeb,

3.2.2. Аттестационная контрольная работа №2

1. Команды удаленного выполнения, Sendmail и электронная почта. Атаки на открытые системы
2. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.
3. Этапы реализации и уровни атак.
4. Атаки с использованием сетевых протоколов.
5. Обеспечение информационной безопасности в открытых системах.
6. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
7. Разработка Политики безопасности для открытых систем.
8. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.

3.2.3. Аттестационная контрольная работа №3

1. Аутентификация субъектов и объектов взаимодействия в открытых системах.
2. Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа. Анализ типовой модели аутентификации.
3. Виртуальные вычислительные сети.
4. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, RemoteAccess VPN.
5. Межсетевые экраны.

6. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений.
7. Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны. Сетевой сканер XSpider. Система обнаружения вторжений Cisco IPS.

3.3. Оценочные средства для проведения итоговой формы контроля

Перечень вопросов на экзамен

1. Стандартизация и модельное представление открытых информационных систем.
2. Роль стандартов в технологии открытых систем.
3. Основные группы стандартов и организации по стандартизации.
4. Модель OSI и POSIX. Интранет как открытая система.
5. Разработка и управление Политикой использования ресурсов интранета.
6. Уязвимость открытых систем на примере интранета
7. Анализ угроз ИБ ресурсам интранета и причины их реализации.
8. Уязвимости операционных систем, серверов, рабочих станций, каналов связи.
9. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, WorldWideWeb,
10. Команды удаленного выполнения, Sendmail и электронная почта. Атаки на открытые системы
11. Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети.
12. Этапы реализации и уровни атак.
13. Атаки с использованием сетевых протоколов.
14. Обеспечение информационной безопасности в открытых системах.
15. Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408.
16. Разработка Политики безопасности для открытых систем.
17. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление.
18. Аутентификация субъектов и объектов взаимодействия в открытых системах.
19. Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа. Анализ типовой модели аутентификации.
20. Виртуальные вычислительные сети.
21. Виды ВЧВС в зависимости от решаемых задач: Intranet VPN, Client/server VPN, Extranet VPN, RemoteAccess VPN.
22. Тема 8. Межсетевые экраны.
23. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений.
24. Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны. Сетевой сканер XSpider. Система обнаружения вторжений Cisco IPS.

Примерные тестовые вопросы

1. Что означает аббревиатура ИБ?

a) Информационное Безопасность
b) Инскрипто Безопасность
c) Инструкция Безопасности

d) Информационный Блок

2. Какое понятие соответствует определению "информация, не предназначенная для всеобщего ознакомления"?
a) Открытая информация
b) Закрытая информация
c) Хакерская информация
d) Исключительная информация

3. Какие приемы могут использоваться злоумышленниками для взлома паролей?
a) Словарные атаки
b) Нагревание системного блока
c) Отправка вредоносных писем
d) Использование определенных звуковых волн

4. Что такое фишинг?
a) Атака на информационную систему, в результате которой данные становятся недоступными
b) Оповещение пользователей о возможных угрозах ИБ
c) Атака на пользователей, направленная на получение конфиденциальных данных
d) Хакерская атака, в результате которой система становится более защищенной

5. Какие из перечисленных угроз в статье "Угрозы безопасности" наиболее важны с точки зрения избежания рисков?
a) Размещение ссылок на вредоносные сайты
b) Электронный взлом
c) Нарушение конфиденциальности персональной информации
d) Внедрение вирусов на компьютеры

6. Что означает термин "вредоносное ПО"?
a) Программное обеспечение, наносящее вред компьютерной системе
b) Программное обеспечение, защищающее компьютерную систему
c) Программа для создания электронной почты
d) Программа для резервного копирования данных

7. Какое основное преимущество использования фаервола?
a) Защита от спама и вирусов
b) Блокирование нежелательных сайтов
c) Контроль над исходящим и входящим трафиком в сети
d) Ускорение работы сети

8. Что такое скимминг?
a) Способ использования чужой кредитной карты
b) Способ получения доступа к Wi-Fi сети
c) Способ перехвата данных с банковских карт
d) Способ защиты операционной системы компьютера

9. Что такое шифрование?
a) Процесс передачи данных по каналу связи
b) Процесс преобразования исходных данных в непонятный для человека вид с помощью алгоритма шифрования
c) Способ блокирования доступа к сайту
d) Способ взлома пароля

10. Как называется вредоносный код, написанный для проявления вредоносной деятельности на целевой системе?
a) Вирус
b) Червь
c) Троян
d) Кейлоггер

11. В чем заключается угроза инъекции?
a) Возможности злоумышленников выполнения своего кода на сервере
b) Способности злоумышленников получения доступа к базам данных
c) Возможности злоумышленников извлечения пароля к веб-ресурсу
d) Возможности злоумышленников осуществления DDoS-атаки

12. Какие меры безопасности необходимы для защиты персональной информации пользователей?
a) Установка антивирусного программного обеспечения
b) Контроль доступа к информации
c) Резервное копирование данных
d) Исключение возможности использования устройств с средствами фиксации видео и аудио разговоров в местах, где эта информация может быть скомпрометирована

13. Что такое DDoS-атака?
a) Атака на сайт с целью изменения информации на нём
b) Атака на доменное имя
c) Атака на сервер, направленная на сбой в его работе
d) Атака на сервер, направленная на перегрузку его канала связи

14. Что такое метод защитного кодирования?
a) Способ приватизации личной информации
b) Способ преобразования информации в вид, доступный только после расшифровки
c) Способ сохранения исходной информации
d) Способ передачи информации без риска ее перехвата

15. Что такое система мониторинга в области ИБ?
a) Способность системы реагировать на попытки несанкционированного доступа к ресурсу
b) Анализ движения денежных средств в банковских системах
c) Программные и аппаратные средства, используемые для сбора и анализа информации о программировании
d) Инструмент для сбора данных о состоянии ИБ системы и активности хакеров.

Ключи

1) A
2) B
3) A
4) C
5) C
6) A
7) C
8) C
9) B
10) C
11) A
12) B
13) D
14) B
15) D

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.

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 невозможно 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).