МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____ А.В. Замятин
«_02_» ____11____ 2021 г.

Фонд оценочных средств по дисциплине

Введение в компьютерную безопасность

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности  В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности  С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор  С.П. Сущенко

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1. Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности	ОР-1.1.2. **Знать**: понятия информации, информационной безопасности, основы государственной информационной политики	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения	ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и	ОР-8.1.3. **Знать**: основные формы, методы и приемы научного исследования при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Высокий уровень знаний; способность самостоятельного анализа проблем предметной	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

безопасности компьютерных систем и сетей	зарубежного опыта по проблемам компьютерной безопасности.		области.			
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.	ОР-9.1.1. **Знать**: угрозы информационной безопасности и меры противодействия им. ОР- ОР-9.1.2. **Знать**: основные средства и способы обеспечения информационной безопасности. ОР-9.1.3. **Знать**: назначение, основные возможности, принципы построения компьютерных систем и сетей.	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.
ОПК-18. Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы	ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности.	ОР-18.1.1. **Знать**: методики анализа безопасности компьютерных систем и сетей	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

ОПК-20. Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ИОПК-20.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания защищенности компьютерных систем.	ОР-20.1.1. **Знать**: виды и назначение стандартов оценивания защищенности компьютерных систем и сетей.	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Основы компьютерных систем и сетей.	ОР-9.1.3 ОР-9.1.3. Знать: назначение, основные возможности, принципы построения компьютерных систем и сетей.	проект
2.	Понятия и задачи компьютерной безопасности.	ОР-1.1.2 ОР-1.1.2. Знать: понятия информации, информационной безопасности, основы государственной информационной политики	проект
3.	Стандарты и нормативные документы компьютерной безопасности	ОР-20.1.1 ОР-20.1.1. Знать: виды и назначение стандартов оценивания защищенности компьютерных систем и сетей.	проект
4.	Механизмы и средства защиты компьютерных систем и сетей.	ОР-9.1.1, ОР-9.1.2 ОР-9.1.1. Знать: угрозы информационной безопасности и меры противодействия им. ОР- ОР-9.1.2. Знать: основные средства и способы обеспечения информационной безопасности.	проект
5.	Защита информации в компьютерных системах и сетях.	ОР-9.1.1, ОР-9.1.2, ОР-8.1.3, ОР-18.1.1 ОР-9.1.1. Знать: угрозы информационной безопасности и меры противодействия им. ОР-9.1.2. Знать: основные средства и способы обеспечения информационной безопасности. ОР-8.1.3. Знать: основные формы, методы и приемы научного исследования при проведении разработок в	проект

		области обеспечения безопасности компьютерных систем и сетей ОР-18.1.1. Знать: методики анализа безопасности компьютерных систем и сетей	

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

Проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине осуществляется в рамках проектного обучения. Формируются команды по 3-5 студентов для совместной групповой работы, которая заключается в реализации проекта в области специальности “Компьютерная безопасность”. В ходе работы над проектом команде студентов требуется выполнить доклад с заявкой на проект, обзорный доклад по предметной области, выполнить промежуточные отчеты о проделанной работе, провести финальную защиту проекта. В зависимости от темы проекта ключевым действием может быть администрирование средств защиты информации, разработка средств защиты информации, анализ безопасности компьютерной системы или сети. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам. Промежуточная аттестация осуществляется на основе защиты проекта.

Типовые варианты проектов

1) Тема проекта - Анализ защищенности компьютерных систем и сетей с использованием сканеров безопасности

- Направления проектной деятельности - Оценивание уровня безопасности компьютерных систем и сетей
- Преимущественный вид деятельности - установка и настройка параметров специализированного программного обеспечения
- Предметная область, приобретаемые знания/умения/навыки (что потребуется изучить) - принципы построения компьютерных систем и сетей; принципы организации, состав и схемы работы операционных систем, криптографические протоколы; модели безопасности компьютерных систем; методы обработки данных мониторинга безопасности компьютерных систем; порядок создания и структура отчета, создаваемого по результатам проверок; нормативные правовые акты в области защиты информации; Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

Обзорный доклад по теме проекта включает:

- Необходимые понятия предметной области (протокол, порт, пакет и т.п.)
- Способы анализа защищенности компьютерных систем и сетей

- Обзор отечественных и зарубежных сканеров безопасности

В ходе промежуточных отчетов и защиты проекта демонстрируются приобретаемые знания/умения/навыки, в частности на базе выбранных сканеров безопасности с использованием пробной версии объясняются методы анализа, реализуемые этим сканерами, показываются возможности сканеров на тестовых примерах, возможности интеграции сканеров с системами управления информационной безопасностью.

Другой вариант работы над проектом: команда делится на две группы, одна из которых защищает компьютерную систему, настраивая необходимые средства защиты, а другая проводит аудит работы первой с использованием сканеров безопасности, пытаясь найти “бреши” в защите.

2) Тема проекта - Разработка средства криптографической защиты информации

- Направления проектной деятельности - Разработка средств защиты информации
- Преимущественный вид деятельности – разработка и тестирование специализированного программного обеспечения
- Предметная область, приобретаемые знания/умения/навыки (что потребуется изучить) - методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных; принципы построения систем защиты информации компьютерных систем; методологии и технологии разработки программного обеспечения; криптографические алгоритмы и особенности их программной реализации; нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации.

Возможный функционал средства криптографической защиты информации (одно из):

- обеспечение юридической значимости электронных документов при обмене
- обеспечение конфиденциальности и контроля целостности информации
- контроль целостности системного и прикладного программного обеспечения
- выработка случайных и псевдослучайных чисел, сессионных ключей шифрования

Обзорный доклад по теме проекта включает:

- Необходимые понятия предметной области (имитовставка, цифровая подпись и пр.)
- Обзор средств криптографической защиты информации
- Реализуемый криптографический(ие) алгоритм(ы)
    - Алгоритм выработки значения хэш-функции
    - Алгоритм формирования и проверки электронной подписи
    - Алгоритм зашифрования/расшифрования данных и вычисление имитовставки

В ходе промежуточных отчетов и защиты проекта демонстрируются “следы” работы команды в системе управления проектом с распределение ролей в IT-команде:

руководитель проекта, аналитик, архитектор, разработчик, дизайнер, тестировщик, системный администратор. Возможно выпадение и/или совмещение ролей, а также то, что одну роль выполняет несколько человек. Например, руководитель проекта - он же архитектор. Разработчик может быть и тестировщиком или администратором. Важная роль - руководитель проекта, который формулирует и раздает задачи остальным членам команды в ходе выполнения всего проекта, производит контроль выполнения задач.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль успеваемости по дисциплине осуществляется на базе оценки докладов (заявка на проект, обзорный доклад предметной области, промежуточный отчет). Доклады оцениваются по бинарной системе (зачет/незачет): зачет – команда в целом удовлетворительно разбирается в выбранной теме проекта, знает материал, отвечает на вопросы с замечаниями или с негрубыми ошибками; незачет – команда слабо разбирается в выбранной теме проекта, плохо знает материал, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Зачет по дисциплине – команда овладела материалом по выбранной теме проекта, возможно с некоторыми недостатками, а также на финальной защите проекта продемонстрировала приобретенные в ходе выполнения проекта высокие/хорошие знания/умения/навыки по теме проекта. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам.

Незачет по дисциплине – команда не прошла текущий контроль успеваемости по дисциплине, а также на финальной защите проекта продемонстрировала низкий уровень знаний/умений/навыков по теме проекта. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам.