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_» ____июля_____ 2021 г.

Фонд оценочных средств по дисциплине

Защита в операционных системах

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил(и):

ассистент кафедры компьютерной безопасности О.В. Брославский

Рецензент:
канд. техн. наук, доцент,
заведующий кафедры 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-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	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; ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и	ОР-1 Знать средства и методы хранения и передачи аутентификационной информации. ОР- 2 Знать защитные механизмы и средства обеспечения безопасности операционных систем.	В совершенстве знает средства и методы хранения и передачи аутентификационной информации. В совершенстве знает защитные механизмы и средства обеспечения безопасности операционных систем.	Знает средства и методы хранения и передачи аутентификационной информации. Знает защитные механизмы и средства обеспечения безопасности операционных систем.	Знает основные средства и методы хранения и передачи аутентификационной информации. Знает основные защитные механизмы и средства обеспечения безопасности операционных систем.	Не знает основные средства и методы хранения и передачи аутентификационной информации. Не знает защитные механизмы и средства обеспечения безопасности операционных систем.

каналам, сетей и систем передачи информации.	системах управления базами данных.					
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях.	ОР-3 Знать требования к подсистеме аудита и политике аудита. ОР-4 Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. ОР-5 Уметь осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.	В совершенстве знает требования к подсистеме аудита и политике аудита. В совершенстве умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. В совершенстве умеет осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.	Знает требования к подсистеме аудита и политике аудита. Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. Умеет осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.	Знает основные требования к подсистеме аудита и политике аудита. Умеет формулировать и настраивать политику безопасности основных операционных систем. Умеет осуществлять меры противодействия основным нарушениям безопасности с использованием различных программных	Не знает требования к подсистеме аудита и политике аудита. Не умеет формулировать и настраивать политику безопасности основных операционных систем. Не умеет осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты

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; ИОПК-18.2 Оценивает соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; ИОПК-18.3 Составляет и оформляет аналитический отчет по результатам проведенного анализа, разрабатывает предложения по устранению выявленных уязвимостей.	ОР-6 Владеть навыками оценки уровня защиты операционных систем. ОР-7 Владеть навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	В совершенстве владеет навыками оценки уровня защиты операционных систем. В совершенстве владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	Владеет навыками оценки уровня защиты операционных систем. Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	Слабо владеет навыками оценки уровня защиты операционных систем. Слабо владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	Не владеет навыками оценки уровня защиты операционных систем. Не владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.

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.	Управление доступом в ОС	ОР 1-7	Лабораторные работы, теоретические вопросы
2.	Методы идентификации и аутентификации в ОС	ОР 1-7	Лабораторные работы, теоретические вопросы
3.	Метода аудита ОС	ОР 1-7	Лабораторные работы, теоретические вопросы

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

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

Примеры лабораторных работ:

1. Реализация управления доступом в ОС Linux при помощи AppArmor.
2. Реализация управления доступом в ОС Linux при помощи SELinux.
3. Реализация собственного модуля аутентификации пользователей (PAM) для ОС Linux.
4. Настройка аудита ОС Linux на примере Auditd.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Примеры тем для теоретических вопросов в устном зачёте:

- Система PAM. Архитектура, принцип работы.
- Система AppArmor. Архитектура, принцип работы
- Система SELinux. Архитектура, принцип работы
- Подсистемы ядра LSM. Архитектура, принцип работы, существующие модули
- Система хранения ключевой информации AF-merge
- Подсистема ядра dm-crypt. LUKS

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

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

Критерием выполнения студентом лабораторной работы является:

- наличие у студента программной реализации механизма защиты или аудита, рассматриваемого в рамках лабораторной работы;
- способность студента объяснить суть механизма защиты, его ограничения и модель нарушителя, в рамках которой данный механизм является эффективным.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме устного зачета по теоретическому материалу.

К зачету допускаются только студенты, успешно выполнившие все, предусматриваемые курсом лабораторные работы.

Каждый билет для устного зачёта состоит из двух теоретических вопросов по двум темам дисциплины.