

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Защита в операционных системах

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Треньяев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

ОПК-18 Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы.

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.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

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

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

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 системах управления базами данных

ИПК-3.1 Разработка технических заданий, эскизных, технических и рабочих проектов работ по защите информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторная работа;

Список лабораторных работ (ИОПК-9.1, ИОПК-9.2, ИОПК-16.1, ИОПК-16.2, ИОПК-16.3, ИОПК-18.1, ИОПК-18.2, ИОПК-18.3, ИПК-3.1)

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.

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.

Результаты лабораторных работ определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Планируемые результаты обучения	Критерии оценивания результатов обучения			
	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
1. Знать средства и методы хранения и передачи аутентификационной информации. 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.
3. Знать требования к подсистеме аудита и политике аудита. 4. Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе.	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	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	Знает основные требования к подсистеме аудита и политике аудита. Умеет формулировать и настраивать политику безопасности основных операционных систем. Умеет осуществлять меры противодействия нарушениям безопасности с использованием различных	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

5. Уметь осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.	осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.	использованием различных программных и аппаратных средств защиты.	программных	защиты
6. Владеть навыками оценки уровня защиты операционных систем.	В совершенстве владеет навыками оценки уровня защиты операционных систем.	Владеет навыками оценки уровня защиты операционных систем.	Слабо владеет навыками оценки уровня защиты операционных систем.	Не владеет навыками оценки уровня защиты операционных систем.
7. Владеть навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	В совершенстве владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	Слабо владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.	Не владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет с оценкой проводится в устной (или письменной) форме по билетам. Билет содержит два теоретических вопроса по двум темам дисциплины. Продолжительность зачета с оценкой 1 час.

Обучающийся должен знать методы защиты информации в современных операционных системах. Уметь продемонстрировать на практике способы обеспечения различных аспектов безопасности ОС на примере выполненных в семестре лабораторных работ. При этом положительная оценка («отлично», «хорошо», «удовлетворительно») ставится, если студент выполнил все лабораторные работы на оценку не ниже «удовлетворительно» и владеет большей частью теоретического материала. Оценка «неудовлетворительно» ставится, если студент не выполнил все лабораторные работы и не освоил большую часть теоретического материала.

Темы для теоретических вопросов на зачете (ИОПК-9.1, ИОПК-9.2, ИОПК-16.1, ИОПК-16.2, ИОПК-16.3, ИОПК-18.1, ИОПК-18.2, ИОПК-18.3, ИПК-3.1)

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

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы (ИОПК-9.1, ИОПК-9.2, ИОПК-16.3, ИОПК-18.1):

1. Понятие защищенной операционной системы.
2. Какие вы знаете защитные механизмы и средства обеспечения безопасности операционных систем?
3. Разграничение доступа в операционных системах.
4. Перечислите методы хранения и передачи аутентификационной информации.
5. Объясните понятие аудита

Теоретические вопросы для проверки остаточных знаний предполагают краткое раскрытие основного содержания соответствующего вопроса.

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент кафедры компьютерной безопасности.