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

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

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

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах.

ПК-2 Способен проводить анализ эффективности программно-аппаратных средств защиты информации в операционных системах.

ПК-3 Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.4.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания безопасности компьютерных систем и сетей.

ИОПК-1.4.2 Определяет уровень защищенности компьютерных систем и сетей и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-1.4.3 Оценивает соответствие механизмов безопасности требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ИПК-1.1 Определяет состав применяемых программно-аппаратных средств защиты информации в операционных системах.

ИПК-1.2 Оценивает угрозы безопасности информации операционных систем.

ИПК-1.3 Противодействует угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем.

ИПК-2.1 Проводит мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах.

ИПК-2.2 Оценивает оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

ИПК-3.1 Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2 Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3 Разрабатывает предложения по совершенствованию системы управления защитой информации.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторная работа;

Список лабораторных работ (ИОПК-1.4.1, ИОПК-1.4.2, ИОПК-1.4.3, ИПК-1.1, ИПК-1.2, ИПК-1.3, ИПК-2.1, ИПК-2.2, ИПК-3.1, ИПК-3.2, ИПК-3.3)

1. Лабораторная работа «Реализация управления доступом в ОС Linux при помощи AppArmor»

Цель: ознакомиться с механизмом контроля доступа в Linux через использование AppArmor, рассмотреть его особенности и способы применения для повышения безопасности системы. В лабораторной работе студенты изучат, как AppArmor позволяет ограничивать действия приложений в соответствии с определёнными профилями безопасности. Практическая часть включает настройку и управление профилями AppArmor, создание новых профилей для заданных приложений и оценку их влияния на безопасность системы.

2. Лабораторная работа «Реализация управления доступом в ОС Linux при помощи SELinux»

Цель: изучить систему контроля доступа SELinux для реализации многоуровневой защиты в операционной системе Linux. В данной лабораторной работе студенты знакомятся с концепциями SELinux, такими как политики безопасности, контексты безопасности, а также режимы работы (Enforcing, Permissive, Disabled). Практическая часть связана с настройкой и управлением политиками SELinux, анализе логов и исправлении проблем, связанных с доступом в различных режимах работы.

3. Лабораторная работа «Реализация собственного модуля аутентификации пользователей (PAM) для ОС Linux»

Цель: научиться создавать и интегрировать собственный модуль аутентификации в систему модульной аутентификации (PAM) для управления доступом пользователей в Linux. Студенты знакомятся с архитектурой PAM, изучают процесс аутентификации, авторизации, учёта и управления сессиями в Linux. Практическая часть включает разработку и развертывание пользовательского модуля PAM, который реализует специфические требования к аутентификации и интеграцию этого модуля в существующую конфигурацию системы.

4. Лабораторная работа «Настройка аудита ОС Linux на примере Auditd».

Цель: ознакомиться с процессом настройки и управления системой аудита в Linux с использованием Auditd для мониторинга и анализа событий системы. Студенты изучают возможности Auditd для записи и анализа событий, что предоставляет возможность контроля и проверки изменений в системе. Практическая часть включает настройку правил аудита, анализ результатов логирования, а также создание отчетов об активности пользователей и процессов для последующего их рассмотрения.

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	В совершенстве знает средства и методы хранения и передачи аутентификационной информации. В совершенстве знает защитные механизмы и средства	Знает средства и методы хранения и передачи аутентификационной информации. Знает защитные механизмы и средства обеспечения безопасности	Знает основные средства и методы хранения и передачи аутентификационной информации. Знает основные защитные механизмы и средства обеспечения безопасности	Не знает основные средства и методы хранения и передачи аутентификационной информации. Не знает защитные механизмы и средства обеспечения безопасности

механизмы и средства обеспечения безопасности операционных систем.	обеспечения безопасности операционных систем.	операционных систем.	операционных систем.	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. 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
6. Владеть навыками оценки уровня защиты операционных систем. 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.

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-1.4.1, ИОПК-1.4.2, ИОПК-1.4.3, ИПК-1.1, ИПК-1.2, ИПК-1.3, ИПК-3.1, ИПК-3.3)

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-1.4.1, ИОПК-1.4.2, ИОПК-1.4.3, ИПК-1.1, ИПК-1.2, ИПК-3.1):

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.