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

Введение в специальность

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. Тренькаев

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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

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

ОПК-20 Способен проводить тестирование и использовать средства верификации механизмов защиты информации.

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

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.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности

ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности

ИОПК-20.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания защищенности компьютерных систем

ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и зарубежного опыта по проблемам компьютерной безопасности

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

## 2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– проекты.

Проведение текущего контроля успеваемости 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.

При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов достижения компетенций: ИОПК-1.1, ИОПК-18.1, ИОПК-20.1, ИОПК-8.1, ИОПК-9.1.

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: 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
- 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: 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:

- 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
- Обзор средств криптографической защиты информации
- Реализуемый криптографический алгоритм
    - Алгоритм выработки значения хэш-функции
    - Алгоритм формирования и проверки электронной подписи
    - Алгоритм зашифрования/расшифрования данных

В ходе промежуточных отчетов и защиты проекта демонстрируются приобретаемые знания/умения/навыки (см. выше), а также цифровые “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 может быть и архитектором, а разработчик может быть и администратором. Важная роль - руководитель проекта, который формулирует и раздает задачи остальным членам команды в ходе выполнения всего проекта, производит контроль выполнения задач.

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.

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

Проведение 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 следующие задачи: 1) выбрать тему проекта, сделать доклад с заявкой на проект, совместно с преподавателем определиться с формой проведения проекта, целью и задачами проекта; 2) изучить выбранный объект защиты, а также механизмы его защиты, сделать обзорный доклад по предметной области проекта; 3) выполнить промежуточные отчеты о проделанной работе, а также провести финальную защиту проекта. Промежуточная аттестация осуществляется на основе защиты проекта.

При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов достижения компетенций: ИОПК-1.1, ИОПК-18.1, ИОПК-20.1, ИОПК-8.1, ИОПК-9.1.

Критерии оценивания промежуточной аттестации:

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.

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

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

– Охарактеризовать область профессиональной деятельности специалиста по безопасности компьютерных систем и сетей.

– Охарактеризовать объекты профессиональной деятельности специалиста по безопасности компьютерных систем и сетей.

– Охарактеризовать виды профессиональной деятельности специалиста по безопасности компьютерных систем и сетей.

– Охарактеризовать трудовые функции специалиста по безопасности компьютерных систем и сетей.

### Информация о разработчиках

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.