

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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:

Директор



А. В. Замятин

« 19 » мая 20 22 г.

Рабочая программа дисциплины

Введение в компьютерную безопасность

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

2022


Код дисциплины в учебном плане: Б1.О.03.04

СОГЛАСОВАНО:

Руководитель ОП

 В.Н. Тренькаев

Председатель УМК

 С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

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-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.

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

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

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

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

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.

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.

2. Задачи освоения дисциплины

– дать представление об области, объектах и видах профессиональной деятельности, в том числе ознакомить с трудовыми функциями специалиста по безопасности компьютерных систем и сетей.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль "Общие вопросы компьютерной безопасности".

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Третий семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Информатика, Архитектура вычислительных систем, Дискретная математика, Языки программирования, Основы информационной безопасности.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:
-лекции: 32 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Основы компьютерных систем и сетей.

- Принципы организации компьютерных сетей.
- Принципы построения современных операционных систем.

Тема 2. Понятия и задачи компьютерной безопасности.

- Основные понятия компьютерной безопасности.
- Атаки на компьютерные системы и сети.

Тема 3. Стандарты и нормативные документы компьютерной безопасности.

- Руководящие документы Гостехкомиссии России.
- Отраслевые стандарты в области информационной безопасности.

Тема 4. Механизмы и средства защиты компьютерных систем и сетей.

- Основные механизмы защиты компьютерных систем и сетей.
- Средства защиты информации компьютерных систем и сетей.

Тема 5. Защита информации в компьютерных системах и сетях.

- Обслуживание средств защиты информации в компьютерных системах и сетях
- Администрирование средств защиты информации в компьютерных системах и сетях
- Оценка уровня безопасности компьютерных систем и сетей
- Разработка средств защиты информации компьютерных систем и сетей

9. Текущий контроль по дисциплине

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.

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 приобретаемые знания/умения/навыки (см. выше), а также цифровые “следы” работы команды в системе управления проектом с распределением 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.

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.

10. Порядок проведения и критерии оценивания промежуточной аттестации

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. 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.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - <https://moodle.tsu.ru/course/view.php?id=6168>

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

в) Методические указания по организации самостоятельной работы студентов.

При разработке проекта следует использовать следующую типовую схему описания проекта: название; описание проблемы; цель проекта; задачи проекта; содержание деятельности; срок реализации проекта; ожидаемые результаты проекта; ресурсы проекта; возможные риски проекта. При разработке проекта нужно: соизмерять желания и возможности; подумать над тем, чего вы действительно хотите добиться; интересоваться мнениями участников проекта; честно планировать своё время и делать всё в свое время. Проект реализуется в несколько этапов, в целом аналогичных этапам подготовки научного исследования и квалификационной работы: выбор темы; разработка и организация плана проекта; осуществление запланированной проектной деятельности; презентация проекта; оценка и анализ результатов.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Нестеров С.А. Основы информационной безопасности: учебное пособие. – М: Лань, 2019, 324 с.

– Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие. – М: ИНФРА-М, 2019, 202 с.

– Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. – М: ИНФРА-М, 2020, 327 с.

– Шаньгин В.Ф. В. Комплексная защита информации в корпоративных системах: учебное пособие. – М: ИНФРА-М, 2015, 590 с.

б) дополнительная литература:

– Галатенко В.А. Основы информационной безопасности: учебное пособие. – М: Интернет-Университет Информационных Технологий, 2010, 205 с.

– Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации- М.: Юрайт, 2016, 308 с.

– Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. -М.: Академия, 2009, 271 с.

в) ресурсы сети Интернет:

– Банк данных угроз безопасности информации ФСТЭК России- <https://bdu.fstec.ru/>

– National Vulnerability Database (NVD) - <https://nvd.nist.gov/>

– Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL:

<http://www.intuit.ru/studies/courses/10/10/info>

– Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL:

<http://www.intuit.ru/studies/courses/2259/155/info>

– Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: <http://www.intuit.ru/studies/courses/102/102/info>

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

- ОС Windows/Linux
- Браузер Firefox/Яндекс
- Публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).
- Системы управления проектом (Trello, YouGile и т.п.)

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – <http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system>

– Электронная библиотека (репозиторий) ТГУ – <http://vital.lib.tsu.ru/vital/access/manager/Index>

- ЭБС Лань – <http://e.lanbook.com/>
- ЭБС Консультант студента – <http://www.studentlibrary.ru/>
- Образовательная платформа Юрайт – <https://urait.ru/>
- ЭБС ZNANIUM.com – <https://znanium.com/>
- ЭБС IPRbooks – <http://www.iprbookshop.ru/>

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации. Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

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