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

Рабочая программа дисциплины

Основы информационной безопасности

по направлению подготовки

02.03.03 Математическое обеспечение и администрирование информационных систем

Направленность (профиль) подготовки:
DevOps-инженерия в администрировании инфраструктуры ИТ-разработки

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
С.П. Сущенко

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения.

ПК-2 Способен проектировать базы данных, разрабатывать компоненты программных систем, обеспечивающих работу с базами данных, с помощью современных инструментальных средств и технологий.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Обладает необходимыми знаниями в области информационных технологий и программных средств

ИОПК-3.2 Применяет знания, полученные в области информационных технологий и программных средств, при решении задач профессиональной деятельности

ИПК-2.3 Использует средства СУБД для выявления проблем производительности при выполнении и повышением пропускной способности базы данных

2. Задачи освоения дисциплины

– Освоить понятийный аппарат информационной безопасности.
– Получить представление о базовых понятиях и задачах криптографии.
– Получить представление о средствах и методах информационной безопасности.
– Ознакомиться с государственной политикой РФ в сфере информационной безопасности, основными механизмами защиты от несанкционированного доступа и базовыми средствами защиты компьютерных сетей.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в модуль Модуль «Самоорганизация и саморазвитие».

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

Второй семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: информатика, дискретная математика.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:
-лекции: 32 ч.
в том числе практическая подготовка: 0 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Информация как объект защиты.

Понятие об информации. Уровни представления информации. Свойства защищаемой информации. Виды тайн. Правовой режим информационных ресурсов.

Тема 2. Понятийный аппарат информационной безопасности.

Виды, способы, замысел, объект, техника защиты информации. Виды нарушителя и классификация угроз.

Тема 3. Государственная политика информационной безопасности.

Государственная система обеспечения информационной безопасности. Законодательная основа обеспечения информационной безопасности. Безопасность критической информационной инфраструктуры РФ. Доктрина информационной безопасности РФ. ФСТЭК.

Тема 4. Угрозы безопасности информации.

Несанкционированные операции с информацией. Перечень типовых угроз. Классификация уязвимостей и угроз. Классификация способов НСД. Типовые атаки на коммуникационные протоколы. Международные базы данных и реестры уязвимостей. Банк данных угроз безопасности информации ФСТЭК России.

Тема 5. Меры противодействия угрозам безопасности.

Правовое обеспечение информационной безопасности. Организационные, физические, технические меры. Политика информационной безопасности организации.

Тема 6. Криптографические методы защиты информации.

Основные задачи криптографии. Криптографические системы. Криптографические протоколы. Цифровая подпись. Хеш-функция. Стандарты в области криптографической защиты информации.

Тема 7. Основные механизмы защиты от несанкционированного доступа.

Контроль целостности. Идентификация. Протоколирование и аудит. Управление доступом. Защита от вредоносных программ. Защита межсетевого взаимодействия. Защита информации при передаче. Предотвращение утечек информации.

Тема 8. Информационная безопасность компьютерных сетей.

Угрозы корпоративной сети. Защита периметра. Основные механизмы защиты. Базовые средства защиты компьютерных сетей (межсетевые экраны, системы анализа защищенности, системы обнаружения атак). Виртуальные частные сети (VPN). Аудит безопасности.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, выполнения контрольных заданий, тестов по лекционному материалу и фиксируется в форме контрольной точки не менее одного раза в семестр.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Порядок проведения промежуточной аттестации. Промежуточная аттестация осуществляется на основе проверки выполнения студентами контрольных заданий и/или

тестов по лекционному материалу и/или по результатам собеседования с использованием перечня контрольных вопросов по курсу. Схема контрольных вопросов соответствует компетентностной структуре дисциплины. При оценивании студенту необходимо продемонстрировать достижение всех запланированных индикаторов.

Критерии оценивания промежуточной аттестации. Зачет по дисциплине проставляется, когда студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении большинства контрольных заданий. Незачет по дисциплине – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении контрольных заданий.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «LMS IDO» - https://lms.tsu.ru/course/view.php?id=31483

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

в) Семинарских / практических занятий по дисциплине нет.

г) Лабораторных работ по дисциплине нет.

д) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах:

- работа со слайдами лекции;
- изучение вопросов, выносимых за рамки лекционных занятий;
- выполнение домашних заданий;
- подготовка к рубежному контролю по теме/разделу

Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым элементом обучения является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы. Контрольные задания, приведенные в планах занятий, выполняются студентами в обязательном порядке.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

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

– Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник. – ИНФРА-М, 2019. – 202 с.

– Е.В. Вострецова Основы информационной безопасности: учебное пособие Издательство Урал.ун-та 2019 г., 204 с.

б) дополнительная литература:

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

– Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов Основы информационной безопасности: учебное пособие. – Горячая линия – Телеком,2006. – 544 с.

– В. В. Бондарев Введение в информационную безопасность автоматизированных систем: учебное пособие. – Издательство МГТУ им. Н. Э. Баумана, 2016. – 250 с.

в) ресурсы сети Интернет:

– Общероссийская Сеть КонсультантПлюс Справочная правовая система. http://www.consultant.ru

– 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:

– Microsoft Office Standart/LibreOffice , браузер Firefox/Яндекс

– публично доступные облачные технологии (Google Docs, Яндекс диск 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/

в) профессиональные базы данных *(при наличии)*:

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

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

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского 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.

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).

15. Информация о разработчиках

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