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» января 2022 г.

Рабочая программа дисциплины

Защита информации на аппаратном уровне

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2022

Код дисциплины в учебном плане: Б1.В.01.01

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ПК-2 – Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

2. Задачи освоения дисциплины

Освоить современные способы защиты т.к. межсетевые экраны, способы безопасных беспроводных соединений и настольных компьютеров, биометрические методы аутентификации и др.

Рассказывается о видах компьютерных атак и о том, как они воздействуют на организацию; приводятся сведения о базовых службах безопасности, используемых для защиты информации и систем, а также о том, как разработать полноценную программу и политики безопасности, о современном состоянии законодательных норм в области информационной безопасности, об управлении рисками и системой безопасности.

3. Место дисциплины в структуре образовательной программы

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

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

Четвертый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: ведение в компьютерную безопасность.

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. Определение информационной безопасности.

Вводится общее понятие информационной безопасности, рассматривается краткая история ее развития. Анализируются современные стандарты обеспечения информационной безопасности. Определяются основные компоненты защиты информации.

Тема 2. Категории атак.

В лекции рассмотрены различные категории атак, даны их определения и условия для их осуществления. Коротко рассмотрен механизм проведения атак.

Тема 3. Методы хакеров.

Лекция посвящена хакерским атакам. Рассмотрена мотивация деятельности хакеров, история методов взлома, различные способы проведения атак. Рассмотрены виды вредоносного ПО, а также способы выявления хакерских атак различных типов.

Тема 4. Службы информационной безопасности.

Рассмотрены основные службы безопасности, проблемы конфиденциальности информации, ее целостности и доступности в компьютерных системах.

Тема 5. Юридические вопросы информационной безопасности.

В лекции рассмотрены юридические вопросы информационной безопасности. Рассмотрено законодательство в данной области ряда стран (США, Австралия, Китай и ряд других). А также вопросы судебного преследования, конфиденциальности личной информации.

Тема 6. Политика.

Рассмотрены вопросы политики информационной безопасности, методика разработки политик, создания, развертывания и эффективного использования.

Тема 7. Рекомендации по обеспечению сетевой безопасности.

Вводится понятие административной безопасности. Даются рекомендации по организации работы службы безопасности на предприятии. Анализируются средства технической безопасности. Рассматриваются плюсы и минусы использования стандарта ISO 17799.

Тема 8. Межсетевые экраны.

В лекции рассмотрены различные типы межсетевых экранов и их различные архитектуры.

Тема 9. Безопасность беспроводных соединений.

Лекция посвящена безопасности беспроводных сетей. Рассмотрены современные беспроводные технологии, вопросы безопасности беспроводных сетей.

9. Текущий контроль по дисциплине

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

10. Порядок проведения и критерии оценивания промежуточной аттестации

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id= 5503

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

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие / Н. И. Синадский. – Екатеринбург: УрГУ, 2008. – 225 с.

– Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.

– Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

б) дополнительная литература:

– Бирюков А.А. Информационная безопасность: защита и нападение / Бирюков А. А. - Москва: ДМК Пресс, 2017. - 434 с.

в) ресурсы сети Интернет:

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

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– 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/

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

Останин Сергей Александрович, заведующий кафедрой компьютерной безопасности, канд. техн. наук, доцент.