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

Защита информации от утечки по техническим каналам

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
2024

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

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.

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.1 Понимает основные физические законы и модели, выявляет естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности

ИОПК-4.2 Применяет соответствующий физико-математический аппарат для формализации, анализа и выработки решения проблем, возникающих в ходе профессиональной деятельности

ИОПК-4.3 Анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники

ИОПК-9.3 Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации

2. Задачи освоения дисциплины

– Освоить основные понятия в области физических явлений и процессов при решении профессиональных задач, познакомиться с основными техническими средствами защиты и особенностями их работы.

– Научиться применению знаний, навыков и умений, необходимых для решения задач инженерно-технической защиты информации с учётом требований системного подхода.

3. Место дисциплины в структуре образовательной программы

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

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в «Модуль «Специализация».

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

Десятый семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Физика», «Основы построения защищённых компьютерных сетей», «Компьютерные сети».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
-лабораторные: 16 ч.
в том числе практическая подготовка: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Системный подход к защите информации.
Рассматриваются основы системного подхода к защите информации.
Тема 2. Основные концептуальные положения
Рассматриваются основные концептуальные положения по защите информации от утечки по техническим каналам.
Тема 3. Информация как предмет защиты
Рассматривается понятие информации как предмета защиты.
Тема 4. Источники опасных сигналов
Рассматриваются основные источники опасных сигналов и их свойства.
Тема 5. Характеристика технической разведки
Обсуждаются основные характеристики технической разведки.
Тема 6. Технические каналы утечки информации
Рассматриваются основные технические каналы утечки информации и их свойства.
Тема 7. Распространение сигналов в технических каналах утечки информации
Тема 8. Подавление опасных сигналов
Тема 9. Средства технической разведки
Тема 10. Аппаратные средства защиты и взлома
Тема 11. Средства радиомониторинга
Тема 12. Средства инженерной защиты и технической охраны объектов
Тема 13. Средства предотвращения утечки информации по техническим каналам
Тема 14. Обнаружители пустот, металлодетекторы
Тема 15 Оптические каналы утечки информации.
Тема 16. Принципы оценки эффективности средств защиты информации от утечки по техническим каналам.

9. Текущий контроль по дисциплине

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

Практическая подготовка оценивается по результатам выполненных лабораторных работ.

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

Зачет в десятом семестре ставится при положительных результатах текущего контроля, положительных ответах на теоретические вопросы и сдаче реферата и доклада по одной из предложенных преподавателем тем. Продолжительность зачета 1 час.

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 системе электронного обучения «IDO»

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

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
– Зайцев А.П. Технические средства и методы защиты информации. -М: Горячая линия-Телеком, 2012 г., 615 с.
– Ищейнов В.Я. Защита конфиденциальной информации. -М: Форум, 2013 г., 256 с.
– Царегородцев А.В. Технические средства защиты информации. Учебник. –М.: Изд. ВГНА Минфина России, 2009.
– Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. -М: ФОРУМ, 2013 г., 592 с.

б) дополнительная литература:

– Хорев А.А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. - М.: Гостехкомиссия России, 1998.

в) ресурсы сети Интернет:

– https://intuit.ru/studies/courses/2291/591/info
– https://samy.pl/magspoof/
– Общероссийская Сеть КонсультантПлюс Справочная правовая система. https://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.).

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.

Лаборатория, оборудованная необходимым комплектом технических средств для защиты информации от утечки по техническим каналам.

15. Информация о разработчиках

Беляев Виктор Афанасьевич, к.т.н., доцент, каф. компьютерной безопасности НИ ТГУ