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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по ОД

_____ Е.В. Луков

«16» сентября 2025 г.

Рабочая программа дисциплины

Защита информации от утечки по техническим каналам

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2026

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-9. Способен применять средства криптографической и технической защитыинформации для решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижениякомпетенций:

ИОПК-9.1. Обладает знанием и демонстрирует навыки применения методов и средств криптографической защиты информации.

ИОПК-9.2. Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам.

2. Задачи освоения дисциплины

– Освоить основные понятия в области физических явлений и процессов при решении профессиональных задач, познакомиться с основными техническими средствамизащиты 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

Шестой 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 утечкипо техническим каналам.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения тестов по лекционному материалу, контроля выполнения лабораторных работ, проверки реферата, 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 шестом семестре проводится 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 LMS IDO.

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

в) Методические указания по выполнению лабораторных работ.

Для выполнения лабораторной работы студенту необходимо:

1. Изучить методические указания по выполнению лабораторной работы.
2. Выполнить работу по предложенному алгоритму действий.
3. Защитить работу преподавателю, ответив на заданные вопросы.

г) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа с материалами лекций; изучение вопросов, выносимых за рамки лекционных занятий; подготовка к лабораторным занятиям; подготовка к рубежному контролю по теме/разделу (аттестации).

Следует целенаправленно, систематически и планомерно работать с конспектами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; консультироваться с преподавателем при возникновении вопросов; активно использоватьучебно-методический комплекс на базе LMS IDO ТГУ.

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.

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием площади и номера помещения в соответствии с документами бюро технической инвентаризации)
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 118 Учебная мебель, оборудование, программное обеспечение: 45 столов по 2 места; 90 стульев; 1 интерактивная доска; Microsoft Windows 10, Microsoft Office 2010. (Лицензия №47729022 от 26.11.2010).	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (78 по паспорту БТИ) Площадь 61,1 м^2.
Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (7 по паспорту БТИ) Площадь 42,3 м^2.

Аудитория № 103 Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core Core i7-8700, AsusTek TUFB360-plus gaming, 16Гб DDR3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022 Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio, Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018) нелинейный локатор «ЦИКЛОН - М1А», локатор-рефлектометр двухпроводных линий «БОР-1», сканирующий приемник AR 8200, оборудование радиодоступа WOP-2ac, Simple Promela Interpreter, ОС Astra Linux Special Edition, Secret Net Studio, ViPNet CSP, JaCarta SecurLogon, IDS/IPS Suricata, Infection Monkey, Wireshark, PfSense, Ntopng, Grype, Metasploit framework, Cisco Packet Tracer, GNS-3, EVE-NG, KatharaFramework, InfoWatch Traffic Monitor.	
Учебная аудитория для самостоятельной работы Аудитория № 103А Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core i7-4790/Ga H97 HD 3/2x 8Gb DDR 3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022 Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio,	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (72 по паспорту БТИ) Площадь 43 м^2.

Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018).	

15. Информация о разработчиках

Беляев Виктор Афанасьевич, канд. техн. наук, доцент, каф. компьютерной безопасности НИ ТГУ.

Вихорь Наталия Анатольевна, канд. физ.-мат. наук, доцент, доцент каф. компьютерной безопасности НИ ТГУ.