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

«__» _____ 2025 г.

Рабочая программа дисциплины

Основы управления информационной безопасностью

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-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

ПК-3. Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-10.1. Понимает принципы формирования политики информационной безопасности в соответствии с нормативными требованиями.

ИОПК-10.2. Умеет организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности на защищаемом объекте.

ИОПК-10.3. Демонстрирует навыки формирования и реализации политики информационной безопасности на защищаемом объекте.

ИПК-3.1. Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2. Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3. Разрабатывает предложения по совершенствованию системы управления защитой информации.

2. Задачи освоения дисциплины

– Изучить и научиться применять основные методологии и практических приемы управления инфраструктурой обеспечения информационной безопасности на предприятии

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

Восьмой семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Основы информационной безопасности, Организационное и правовое обеспечение информационной безопасности, Модели безопасности компьютерных систем, Программно-аппаратные средства защиты информации.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

–лекции: 16 ч.

–практические занятия: 16 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Задачи менеджмента в сфере информационной безопасности.

Задачи управления информационной безопасностью. Понятие безопасной информационной инфраструктуры и ее составляющие. Уровни организационной работы в сфере информационной безопасности.

Тема 2. Управление рисками информационной безопасности.

Основные понятия и определения управления информационными рисками. Процесс управления рисками. Описание внешних и внутренних условий, в которых функционирует организация, определение целей управления рисками, определение критерия оценки и приемлемости риска. Шкала ценности активов. Методы оценки рисков. Шкалы вероятности угроз и уязвимостей. Этапы обработки рисков. Управление информационными рисками, стандарты, нормативные документы, рекомендации.

Тема 3. Управление информационной безопасностью на уровне предприятия

Структура организационной деятельности по обеспечению информационной безопасности на уровне предприятия. Структура политики информационной безопасности и процесс ее разработки. Содержание политики информационной безопасности предприятия. Детализированные политики безопасности. Задачи департамента информационной безопасности. Организационная работа с персоналом.

Тема 4. Управление инцидентами информационной безопасности.

Нормативные документы, регламентирующие аспекты управления инцидентами информационной безопасности. Процедуры и этапы реагирования на инциденты. Локализация и устранение последствий инцидента. Анализ процесса нападения и его обстоятельств.

Тема 5. Аудит состояния информационной безопасности предприятия.

Цель аудита. Этапы аудита информационной безопасности. Методики оценки рисков информационной безопасности. Содержание аудиторской проверки. Понятие инструментального контроля. Содержание отчета о результатах аудита.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проверки контрольных заданий 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

Зачет в восьмом семестре проводится в устной/письменной форме на основе списка контрольных вопросов по дисциплине. Продолжительность зачета с оценкой 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) План семинарских / практических занятий по дисциплине.

–Менеджмент в сфере информационной безопасности

–Правовые основы построения системы защиты информации и оценка рисков

–Мониторинг безопасности и реагирование на инциденты.

–Аудит состояния информационной безопасности предприятия.

–Политика информационной безопасности предприятия.

г) Лабораторных работ по дисциплине нет.

д) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа со слайдами лекции (конспектом); изучение вопросов, выносимых за рамки лекционных занятий; подготовка к рубежному контролю по теме/разделу (аттестации). Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым 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.

12. Перечень учебной литературы и ресурсов сети Интернет

а) Основная литература:

– Мошак Н. Н. Основы управления информационной безопасностью: учебное пособие / Н. Н. Мошак; под редакцией В. В. Овчинникова. — Санкт-Петербург: ГУАП, 2022. – 141 с.

– Основы информационной безопасности: учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва: Горячая линия – Телеком, 2011. – 558 с.

б) Дополнительная литература:

– Нестеров С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров. - 5-е изд., стер. - Санкт-Петербург: Лань, 2019. - 324 с.

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

– Конев А.А., Давыдова Е.М., Шелупанов А.А. Управление информационной безопасностью: лабораторный практикум. – Томск: В-Спектр, 2017. – 122 с.

– Поздняк, И. С. Управление информационной безопасностью: методические указания / И.С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. – 43 с.

в) Ресурсы сети Интернет:

– Национальный портал онлайн обучения «Открытое образование» - https://openedu.ru

– Федеральная служба по техническому и экспортному контролю России - https://fstec.ru/

– Федеральное агентство по техническому регулированию и метрологии (Росстандарт) - https://protect.gost.ru/

13. Перечень информационных технологий

а) Лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office, ОС Windows, Яндекс Браузер

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

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения семинарских / практических занятий, 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.

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 практических занятий и занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 115. Учебная мебель, оборудование, программное обеспечение: 13 столов по 2 места; 26 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 1 системный блок (Intel Core i7-12700K, AsusTek B660M-K D4, 16Гб DDR4); 1 монитор; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Dr.Web Desktop Security Suite, Aktru recorder, Aktru Meet, WinRar. (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018) .	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (29 по паспорту БТИ) Площадь 40,9 м^2.
Учебная аудитория для самостоятельной работы	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (72 по паспорту БТИ)

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, Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018).	Площадь 43 м^2.

15. Информация о разработчиках

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