МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____А.В. Замятин
«_02_» _____ 2021 г.

Введение в компьютерную безопасность

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*очная*
Общая трудоёмкость	*2 з.е.*
Часов по учебному плану	*72*
в том числе:	
аудиторная контактная работа	*33,85*
самостоятельная работа	*38,15*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 3 – зачет*

Томск-2021

Программу составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности С.А.Останин

Рабочая программа дисциплины «Введение в компьютерную безопасность» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Цель освоения дисциплины – формирование представлений об области, объектах и видах профессиональной деятельности, а также ознакомление с трудовыми функциями специалиста по безопасности компьютерных систем и сетей.

1. Место дисциплины в структуре ОПОП

Дисциплина «Введение в компьютерную безопасность» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Общие вопросы компьютерной безопасности».

Для освоения дисциплины необходимо иметь базовые представления о современных информационных технологиях, проблемах информационной безопасности, вычислительной технике и программировании.

Пререквизиты дисциплины: Информатика, Архитектура вычислительных систем, Дискретная математика, Языки программирования, Основы информационной безопасности, Алгоритмы и структуры данных.

Постреквизиты дисциплины: дисциплины модуля “Специализация”

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1. Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности	ОР-1.1.2. **Знать**: понятия информации, информационной безопасности, основы государственной информационной политики
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и зарубежного опыта по проблемам компьютерной безопасности.	ОР-8.1.3. **Знать**: основные формы, методы и приемы научного исследования при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
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	ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.	ОР-9.1.1. **Знать**: угрозы информационной безопасности и меры противодействия им. ОР-9.1.2. **Знать**: основные средства и способы обеспечения информационной безопасности. ОР-9.1.3. **Знать**: назначение, основные возможности, принципы построения компьютерных систем и сетей.

информации от утечки по техническим каналам, сетей и систем передачи информации		
ОПК-18. Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы	ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности.	ОР-18.1.1. **Знать**: методики анализа безопасности компьютерных систем и сетей
ОПК-20. Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ИОПК-20.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания защищенности компьютерных систем.	ОР-20.1.1. **Знать**: виды и назначение стандартов оценивания защищенности компьютерных систем и сетей.

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	Семестр 3	всего
Общая трудоемкость	72	72
Контактная работа:	33,85	33,85
Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)		
Семинары (СЗ)		
Групповые консультации		
Индивидуальные консультации	1,85	1,85
Промежуточная аттестация		
Самостоятельная работа обучающегося:	38,15	38,15
- выполнение проекта	38,15	38,15
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Зачет**	**Зачет**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Основы компьютерных систем и сетей.	Лекции	3		**8**		ОР-9.1.3
1.1.	Принципы организации компьютерных сетей.	Лекции	3		4		
1.2.	Принципы построения современных операционных систем.	Лекции	3		4		
	Раздел 2. Понятия и задачи компьютерной безопасности.	Лекции	3		**8**		ОР-1.1.2
2.1.	Основные понятия компьютерной безопасности.	Лекции	3		4		
2.2.	Атаки на компьютерные системы и сети.	Лекции	3		4		
	Раздел 3. Стандарты и нормативные документы компьютерной безопасности.	Лекции	3		**8**		ОР-20.1.1
3.1.	Руководящие документы Гостехкомиссии России.	Лекции	3		4		
3.2.	Отраслевые стандарты в области информационной безопасности.	Лекции	3		4		
	Раздел 4. Механизмы и средства защиты компьютерных систем и сетей.	Лекции	3		**8**		ОР-9.1.1, ОР-9.1.2.
4.1.	Основные механизмы защиты компьютерных систем и сетей.	Лекции	3		4		
4.2.	Средства защиты информации компьютерных систем и сетей.	Лекции	3		4		
	Раздел 5. Защита информации в компьютерных системах и сетях.	СРС	3		38,15		ОР-9.1.1, ОР-9.1.2, ОР-8.1.3, ОР-18.1.1
5.1.	Обслуживание средств защиты информации в компьютерных системах и сетях	СРС	3		10		
5.2.	Администрирование средств защиты информации в компьютерных системах и сетях	СРС	3		10		
5.3.	Оценивание уровня безопасности компьютерных систем и сетей	СРС	3		10		
5.4.	Разработка средств защиты информации компьютерных систем и сетей	СРС	3		8,15		
	Подготовка к промежуточной аттестации в форме зачета	СРС	3		33,7		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Образовательная технология – курс лекций и проектное обучение. Формируются команды по 3-5 студентов для совместной групповой работы, которая заключается в реализации проекта в области специальности “Компьютерная безопасность”. В ходе работы над проектом команде студентов требуется выполнить следующие задачи: 1) выбрать тему проекта, сделать доклад с заявкой на проект, совместно с преподавателем определиться с формой проведения проекта, целью и задачами проекта; 2) изучить выбранный объект защиты, а также механизмы его защиты, сделать обзорный доклад по предметной области проекта; 3) выполнить промежуточные отчеты о проделанной работе, а также провести финальную защиту проекта. В зависимости от темы проекта ключевым действием может быть администрирование средств защиты информации, разработка средств защиты информации, анализ безопасности компьютерной системы или сети. Оценка за проделанную работу выставляется всей команде, но не отдельным ее участникам. Промежуточная аттестация осуществляется на основе защиты проекта.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Нестеров С.А.	Основы информационной безопасности: учебное пособие	Лань	2019 г, 324 с.
2.	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие	ИНФРА-М	2019 г., 202 с.
3	Хорев П.Б.	Программно-аппаратная защита информации: учебное пособие	ИНФРА-М	2020 г., 327 с.
4	Шаньгин В.Ф. В.	Комплексная защита информации в корпоративных системах: учебное пособие	ИНФРА-М	2015 г., 590 с.
Дополнительная литература				
5.	Галатенко В.А.	Основы информационной безопасности: учебное пособие	Интернет-Университет Информационных Технологий	2010 г., 205 с.
6.	Запечников С.В.,	Криптографические методы	Юрайт	2016 г., 308 с.

	Казарин О.В., Тарасов А.А.	защиты информации		
7.	Черемушкин А.В.	Криптографические протоколы. Основные свойства и уязвимости	Академия	2009 г., 271 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

- Банк данных угроз безопасности информации ФСТЭК России- https://bdu.fstec.ru/
- National Vulnerability Database (NVD) - https://nvd.nist.gov/
- 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

4.3. Перечень лицензионного и программного обеспечения

- ОС Windows/Linux
- Браузер Firefox/Яндекс

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходима лекционная аудитория. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. Методические указания обучающимся по освоению дисциплины

- целенаправленно, систематически и планомерно работать со слайдами лекций;
-изучать рекомендуемую литературу, добывая новые/обобщая полученные знания;
-тратить не менее часа в день на самостоятельную работу;
-консультироваться с преподавателем при возникновении вопросов;
-активно использовать учебно-методический комплекс на базе Moodle ТГУ;
-работать с тематическими форумами в сети Интернет.

6. Преподавательский состав, реализующий дисциплину

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

7. Язык преподавания – русский язык.