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
«_11_» _____ 2021 г.

Основы информационной безопасности

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*02.03.02 Фундаментальная информатика и информационные технологии* *Направленность (профиль) «Искусственный интеллект и разработка программных продуктов»*
Форма обучения	*очная*
Общая трудоёмкость	*3 з.е.*
Часов по учебному плану	*108*
в том числе:	
аудиторная контактная работа	*33.85*
самостоятельная работа	*74.15*
Вид контроля в семестрах	
зачет	*2 семестр – 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 «Основы информационной безопасности» разработана в соответствии с образовательным стандартом высшего образования – бакалавриат, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии (Утвержден Ученым советом НИ ТГУ, протокол от 27.10.2021 г. № 08).

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 о базовых понятиях и задачах, средствах и методах информационной безопасности, государственной политике РФ в сфере информационной безопасности, особенностях обеспечения информационной безопасности в компьютерных сетях.

1. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины», входит в модуль «Самоорганизация и саморазвитие».

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

Пререквизиты дисциплины: «История информатики», «Введение в компьютерные науки».

Постреквизиты дисциплины: «Компьютерные сети», «Операционные системы», «Базы данных».

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

Таблица 1.

Компетенция	**Индикатор универсальной компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-3. Способен к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям	ИОПК-3.1. Использует методы построения и анализа алгоритмов при проектировании и разработке программных систем.	ОР-3.1.1. Знает угрозы информационной безопасности и меры противодействия им. ОР-3.1.2. Владеет понятийным аппаратом информационной безопасности.
	ИОПК-3.2. Использует фундаментальные знания для реализации алгоритмов пригодных для практического применения в области информационных систем и технологий	ОР-3.2.1. Знает основные средства и способы обеспечения информационной безопасности. ОР-3.2.2. Умеет корректно использовать криптографические системы обеспечения безопасности информации. ОР-3.2.3. Знает механизмы и элементы государственной системы обеспечения информационной безопасности.
ПК-2. Способен проектировать базы данных,	ИПК-2.3. Использует средства СУБД для выявления проблем	ОР-2.3.1 Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.

разрабатывать компоненты программных систем, обеспечивающих работу с базами данных, с помощью современных инструментальных средств и технологий	производительности при выполнении и повышением пропускной способности базы данных	

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
Общая трудоемкость	**108**	**108**
Контактная работа:	**33.85**	**33.85**
Лекции	32	32
Групповые консультации	1.6	1.6
Промежуточная аттестация	0.25	0.25
Самостоятельная работа обучающегося:	**74.15**	**74.15**
- *изучение учебного материала, публикаций*	74.15	74.15
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. Информация как объект защиты.		2		**6**	1-6	ОР-3.1.2, ОР-2.3.1
1.1	Понятие об информации. Уровни представления информации.	Лекции	2		1	1-6	ОР-3.1.2
1.2	Свойства защищаемой информации. Виды тайн.	Лекции	2		1	1-6	ОР-2.3.1
1.3	Правовой режим информационных ресурсов.	СРС	2		4	1-6	ОР-3.1.2, ОР-2.3.1
	Раздел 2. Понятийный аппарат информационной безопасности.		2		**8**	1-6	ОР-3.1.1, ОР-3.1.2
2.1	Виды, способы, замысел, объект, техника защиты информации.	Лекции	2		1	1-6	ОР-3.1.2
2.2	Виды нарушителя и классификация угроз.	Лекции	2		1	1-6	ОР-3.1.1
2.3	Банк данных угроз безопасности информации ФСТЭК России.	СРС	2		6	1-6	ОР-3.1.1, ОР-3.1.2
	Раздел 3. Государственная политика информационной безопасности.		2		**10**	1-6	ОР-3.2.3
3.1	Государственная система обеспечения информационной безопасности.	Лекции	2		1	1-6	ОР-3.2.3
3.2	Законодательная основа обеспечения информационной безопасности.	Лекции	2		1	1-6	ОР-3.2.3
3.3	Безопасность критической информационной инфраструктуры РФ.	СРС	2		2	1-6	ОР-3.2.3
3.4	Доктрина информационной безопасности РФ. ФСТЭК.	СРС	2		6	1-6	ОР-3.2.3
	Раздел 4. Угрозы безопасности информации.		2		**12**	1-6	ОР-3.1.1, ОР-3.1.2
4.1	Несанкционированные операции с информацией. Перечень типовых угроз.	Лекции	2		2	1-6	ОР-3.1.1, ОР-3.1.2
4.2	Классификация уязвимостей и угроз. Классификация способов НСД.	Лекции	2		2	1-6	ОР-3.1.1, ОР-3.1.2
4.3	Типовые атаки на коммуникационные протоколы.	СРС	2		2	1-6	ОР-3.1.1, ОР-3.1.2
4.4	Международные базы данных и реестры уязвимостей.	СРС	2		6	1-6	ОР-3.1.1, ОР-3.1.2
	Раздел 5. Меры противодействия угрозам безопасности.		2		**12**	1-6	ОР-3.1.1, ОР-3.1.2
5.1	Правовое обеспечение информационной безопасности.	Лекции	2		1	1-6	ОР-3.1.1, ОР-3.1.2
5.2	Организационные, физические, технические меры.	Лекции	2		1	1-6	ОР-3.1.1, ОР-3.1.2
5.3	Политика информационной безопасности организации.	СРС	2		10	1-6	ОР-3.1.1, ОР-3.1.2
	Раздел 6. Криптографические методы защиты информации.		2		**20**	1-6	ОР-3.2.2
6.1	Основные задачи криптографии. Криптографические системы.	Лекции	2		4	1-6	ОР-3.2.2
6.2	Криптографические протоколы. Цифровая подпись. Хеш-функция.	Лекции	2		4	1-6	ОР-3.2.2
6.3	Стандарты в области криптографической защиты информации.	СРС	2		12	1-6	ОР-3.2.2

	Раздел 7. Основные механизмы защиты от несанкционированного доступа.		2		**18**	1-6	ОР-3.1.1, ОР-3.2.1
7.1	Контроль целостности, идентификация, протоколирование и аудит.	Лекции	2		2	1-6	ОР-3.1.1, ОР-3.2.1
7.2	Управление доступом, защита от вредоносных программ.	Лекции	2		4	1-6	ОР-3.1.1, ОР-3.2.1
7.3	Защита межсетевого взаимодействия, защита информации при передаче, предотвращение утечек информации.	СРС	2		12	1-6	ОР-3.1.1, ОР-3.2.1
	Раздел 8. Информационная безопасность компьютерных сетей.		2		**20.15**	1-6	ОР-3.1.1, ОР-3.2.1
8.1	Угрозы корпоративной сети. Защита периметра. Основные механизмы защиты.	Лекции	2		2	1-6	ОР-3.1.1, ОР-3.2.1
8.2	Базовые средства защиты компьютерных сетей (межсетевые экраны, системы анализа защищенности, системы обнаружения атак и др.).	Лекции	2		4	1-6	ОР-3.1.1, ОР-3.2.1
8.3	Виртуальные частные сети (VPN). Аудит безопасности.	СРС	2		14,15	1-6	ОР-3.1.1, ОР-3.2.1
	Консультации в период теоретического обучения	Консультации	2		1,6		
	Прохождение промежуточной аттестации в форме зачета	З	2		0.25		

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

Основой обучения является курс лекций. Самостоятельная работа студента включает в себя работу с конспектами лекций, выполнение контрольных заданий, подготовку к зачету, изучение литературы. Изучение литературы можно разделить на два вида: изучение базовой литературы, изучение дополнительной литературы. Отдельно следует выделить подготовку к зачету, когда требуется повторить весь учебный курс. Наряду с лекционным материалом для самостоятельной подготовки к зачету следует использовать рекомендуемые учебники (учебные пособия), справочные пособия, научно-образовательные ресурсы сети Интернет, консультации лектора. Учебно-методическое обеспечение для самостоятельной работы студента включает: список основной и дополнительной учебной литературы по курсу; список информационные ресурсов в сети Интернет по курсу; конспекты (слайды) лекционных занятий; перечень контрольных вопросов по курсу. Промежуточная аттестация осуществляется на основе проверки выполнения контрольных заданий и/или по результатам собеседования с использованием перечня контрольных вопросов по курсу.

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».

Информационное обеспечение дисциплины:

1. Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/10/10/info
2. Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/2259/155/info
3. Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/102/102/info

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.	Основы информационной безопасности: учебник	ИНФРА-М	2019 г., 202 с.
Дополнительная литература				
3.	Галатенко В.А.	Основы информационной безопасности: учебное пособие	Интернет-Университет Информационных Технологий	2010 г., 205 с.
4.	Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов	Основы информационной безопасности: учебное пособие	Горячая линия - Телеком	2006 г., 544 с.

5.	Е.В. Вострецова	Основы информационной безопасности: учебное пособие	Издательство Урал.ун-та	2019 г., 204 с.
6.	В. В. Бондарев	Введение в информационную безопасность автоматизированных систем: учебное пособие	Издательство МГТУ им. Н. Э. Баумана	2016 г., 250 с.

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

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

4.3. Перечень лицензионного и программного обеспечения

Не требуется.

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционная аудитория или система управления обучением (виртуальная обучающая среда) с поддержкой видео-конференций. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов.

5. Методические указания обучающимся по освоению дисциплины

- целенаправленно, систематически и планомерно работать с конспектами (слайдами) лекций и литературой;
- изучать литературу на базе конспектирования, добывая новые или обобщая ранее полученные знания;
- при подготовке к зачету источники информации изучать выборочно в соответствии с программой курса, используя оглавление источника и ключевые слова;
- рекомендуется тратить несколько часов в день на самостоятельную работу;
- консультироваться с преподавателем при возникновении проблем при освоении курса (работе с источниками, выполнении заданий и т. п.);
- работать со справочными пособиями и тематическими платформами в сети Интернет.

6. Преподавательский состав, реализующий дисциплину

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

7. Язык преподавания – русский язык.