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_» _июля_ 2021 г.

Защита программ и данных

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 9 – зачет*

Томск-2021

Программу составила:
ассистент кафедры компьютерной безопасности  О.В. Брославский

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

Рабочая программа дисциплины «Защита программ и данных» 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

Цель – теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий; формирование у обучающегося компетенций для научно-исследовательского и эксплуатационного видов деятельности.

1. Место дисциплины в структуре ОПОП

Дисциплина «Защита программ и данных» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: Языки программирования, Операционные системы

Постреквизиты дисциплины: преддипломная практика.

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-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; ИОПК-13.2 Определяет параметры функционирования, архитектуру и интерфейсы компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; ИОПК-13.3 Проводит анализ компонент программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия.	ОР-1 Знать средства и методы хранения и передачи авторизованной информации. ОР-2 Знать защитные механизмы и средства обеспечения безопасности программ и данных.
ОПК-19. Способен оценивать корректность программных реализаций алгоритмов защиты информации	ИОПК-19.1 Обладает знанием формальных приемов, правил, алгоритмов, технологий создания и документирования контрольных примеров и тестовых наборов данных; ИОПК-19.2 Осуществляет подготовку тестовых наборов данных в соответствии с выбранной методикой, а также проверку работоспособности программного обеспечения на основе разработанных тестовых наборов данных;	ОР-3 Уметь осуществлять анализ программного обеспечения на наличия уязвимостей. ОР-4 Уметь проводить дизассемблирование и отладку программного обеспечения.

	ИОПК-19.3 Осуществляет сбор и анализ полученных результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам.	
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; ИОПК-20.2 Проводит исследование механизмов защиты информации, в том числе с использованием средств верификации, и делает выводы по оценке защищенности и доверия.	ОР-5 Владеть навыками оценки уровня защиты программ и данных.
ПК-2. Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей	ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации.	ОР-6 Знать требования к подсистеме аудита и политике аудита. ОР-7 Уметь противодействовать компьютерным атакам и вирусам с использованием антивирусного программного обеспечения.
ПК-3. Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей	ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием ИПК-3.3 Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации	ОР-8 Знать основные средства и методы анализа программных реализаций средств защиты информации ОР-9 Владеть навыками анализа программных реализаций средств защиты информации

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	
	9 семестр	всего
Общая трудоемкость	72	72
Контактная работа:	33,85	33,85
Лекции (Л):		
Практики (ПЗ)	32	32
Лабораторные работы (ЛР)		
Семинары (СЗ)		
Групповые консультации		
Индивидуальные консультации	1,6	1,6
Промежуточная аттестация	0,25	0,25
Самостоятельная работа обучающегося:	38,15	38,15
- подготовка к лабораторным и практическим занятиям	10,9	10,9
- подготовка к рубежному контролю по теме/разделу	27,25	27,25
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
1.	Анализ программных реализаций	Практики	9		10	1, 2	ОР 1-9
2.	Защита программ от изучения	Практики	9		10	1, 2	ОР 1-9
3.	Программные закладки	Практики	9		4	1, 2	ОР 1-9
4.	Внедрение программных закладок	Практики	9		4	1, 2	ОР 1-9
5.	Противодействие программным закладкам	Практики	9		4	1, 2	ОР 1-9
	Подготовка к промежуточной аттестации в форме зачета	СРС	**9**		**1,6**	**1, 2**	
	Прохождение промежуточной аттестации в форме зачета	Э	**9**		**0,25**		

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

- Для освоения дисциплины необходимо регулярное посещение лекций и повторение пройденного материала;
- самостоятельная работа студентов включает повторение пройденного материала и изучение рекомендованных разделов из основной и дополнительной литературы;
- промежуточная аттестация по дисциплине выполняется в виде контрольной работы по освоенному материалу.

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».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Проскурин В.Г.	Защита программ и данных, Учебное пособие	Академия	2011 г., 208 с.
2.	Столяров А.В.	Программирование на языке ассемблера NASM для ОС Unix, Учебное пособие	МАКС Пресс	2011 г., 188 с.
Дополнительная литература				
1.	Юричев, Д.	Reverse Engineering для начинающих	Электронный ресурс	2018 г., 1036 с.

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

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ : [сайт]. – [Томск, 2011–2016]. – URL: http://vital.lib.tsu.ru/vital/access/manager/Index.

4.3. Перечень лицензионного и программного обеспечения

IDA Freeware, QEMU, Oracle VM VirtualBox / VMware Workstation Player или аналогичная система виртуализации.

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения практических занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов, проведения практических занятий и выполнения лабораторных работ.

5. Методические указания обучающимся по освоению дисциплины

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения практических занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов и проведения практических занятий.

6. Преподавательский состав, реализующий дисциплину

Брославский Олег Викторович, ассистент кафедры компьютерной безопасности ТГУ.

7. Язык преподавания – русский язык.