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_» _июня_ 2021 г.

Анализ уязвимостей программного обеспечения

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	*3 з.е.*
Часов по учебному плану	*108*
в том числе:	
аудиторная контактная работа	*67.45*
самостоятельная работа	*40.55*
Вид(ы) контроля в семестрах	
экзамен/зачет/зачет с оценкой	*Семестр 9 – зачет*

Томск-2021

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

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

Рабочая программа дисциплины «Анализ уязвимостей программного обеспечения» 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 – изучение студентом основных видов уязвимостей программного обеспечения; освоение основных методов и средств анализа и устранения уязвимостей программных реализаций.

1. Место дисциплины в структуре ОПОП

Дисциплина «Анализ уязвимостей программного обеспечения» относится к части, формируемой участниками образовательных отношений, 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 основные средства и методы анализа программных реализаций на предмет уязвимостей. ОР-5 Владеть приемами анализа программных реализаций на наличие уязвимостей. ОР-3 Уметь выявлять и устранять уязвимости программных реализаций и локализовать их последствия.
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-2 Знать статические и динамические методы анализы программных реализаций. ОР-4 Уметь проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности.
ПК-2. Способен проектировать и	ИПК-2.3 Осуществляет разработку требований, проектирует и	ОР-6 Знать способы, методы и критерии оценки эффективности реализации систем

разрабатывать средства защиты информации компьютерных систем и сетей	разрабатывает средства защиты информации в соответствии с техническим заданием	защиты информации.

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	9 семестр	всего
Общая трудоемкость	108	108
Контактная работа:	67,45	67,45
Лекции (Л):		
Практики (ПЗ)	16	16
Лабораторные работы (ЛР)	48	48
Семинары (СЗ)		
Групповые консультации		
Индивидуальные консультации	3,2	3,2
Промежуточная аттестация	0,25	0,25
Самостоятельная работа обучающегося:	40,55	40,55
- подготовка к лабораторным и практическим занятиям	17	17
- подготовка к рубежному контролю по теме/разделу	23,55	23,55
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.	Понятие и классификация уязвимостей программного обеспечения	Практики, ЛР	9		2	1, 2	ОР 1-6
2.	Актуальные уязвимости современного программного обеспечения	Практики, ЛР	9		11	1, 2	ОР 1-6
3.	Уязвимости этапа проектирования программного обеспечения	Практики, ЛР	9		11	1, 2	ОР 1-6
4.	Предотвращение уязвимостей на этапе реализации	Практики, ЛР	9		11	1, 2	ОР 1-6
5.	Анализ бинарных уязвимостей программного обеспечения	Практики, ЛР	9		29	1, 2	ОР 1-6
	Подготовка к промежуточной аттестации в форме зачета	СРС	**9**		**3,2**	**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».

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.	Фленов М. Е.	Linux глазами хакера. - 6-е изд.	БХВ	2021, 416 с.
2.	Weidman Georgia	Penetration Testing: A Hands-On Introduction to Hacking	No Starch Press	2014, 528 с.
Дополнительная литература				
4.	Stuttard Dafydd, Pinto Marcus	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws	Wiley	2011 г., 912 с.
5.	Erickson Jon	Hacking: The Art of Exploitation, 2nd Edition	No Starch Press	2008 г., 488 с.
6.				
7.				
8.				

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

Burp Suite, Kali Linux, 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.