

МИНОБРАЗОВАНИЯ 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.

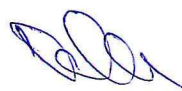


Безопасность веб-приложений

рабочая программа дисциплины

Закреплена за кафедрой	<i>компьютерной безопасности</i>
Учебный план	<i>10.05.01 Компьютерная безопасность, профиль «Анализ безопасности компьютерных систем»</i>
Форма обучения	<i>очная</i>
Общая трудоёмкость	<i>3 з.е.</i>
Часов по учебному плану	<i>108</i>
в том числе:	
аудиторная контактная работа	<i>33,85</i>
самостоятельная работа	<i>74,15</i>
Вид(ы) контроля в семестрах	
экзамен/зачет/зачет с оценкой	<i>Семестр А – зачет</i>

Программу составил:
канд. техн. наук, доцент,
заведующий кафедрой компьютерной безопасности



С.А. Останин

Рецензент:
канд. физ.-мат. наук, доцент,
доцент кафедры компьютерной безопасности



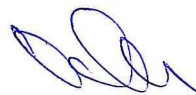
Н.А. Вихорь

Рабочая программа дисциплины «Безопасность веб-приложений» 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 – формирование у студентов знаний об основных типах атак на веб-приложения и методах их предотвращения

Задачи:

- изучить основные элементы и механизмы веб-приложений (протокол HTTP, модель DOM, политика SOP, веб-браузеры, веб-серверы, балансировщики нагрузки);
- изучить основные атаки на веб-приложения: XSS, SQL, CSRF, IDOR и др.
- научить обнаруживать и защищаться от атак рассматриваемых классов.

1. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность веб-приложений» относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: Компьютерные сети, Основы построения защищённых компьютерных сетей

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-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности.	ОР-1. Владеет навыками использования различных программных средств обеспечения информационной безопасности
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 информации от утечки по техническим каналам, сетей и систем передачи информации	ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.	ОР-2. Знает основные виды и источники уязвимостей веб-приложений ОР-3. Знает методы анализа безопасности веб-приложений. ОР-4. Умеет проводить анализ безопасности веб-приложений.
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-5. Знает основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений. ОР-6. Умеет проводить работы по оценке защищенности веб-приложений и

	ИОПК-20.2 Проводит исследование механизмов защиты информации, в том числе с использованием средств верификации, и делает выводы по оценке защищенности и доверия.	составлять отчеты по результатам проведенных работ.
ПК-3. Способен проектировать программно-аппаратные средства защиты информации компьютерных систем и сетей	ИПК-3.3 Проведение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации	ОР-7. Знает порядок проведения аттестации по требованиям 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	
	Семестр А	всего
Общая трудоемкость	108	108
Контактная работа:	33,85	33,85
Лекции (Л):	16	16
Практики (ПЗ)		
Лабораторные работы (ЛР)	16	16
Семинары (СЗ)		
Групповые консультации		
Индивидуальные консультации	1,6	1,6
Промежуточная аттестация	0,25	0,25
Самостоятельная работа обучающегося:	74,15	74,15
- изучение учебного материала, публикаций	54	54
- подготовка к лабораторным занятиям	14	14
- подготовка к промежуточной аттестации в форме зачета	6,15	6,15
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	С е м е с т р	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
1	Архитектура веб-приложений.	Лекции ЛР	10		4	1, 2	ОР 1-7
2	Поиск уязвимостей к атакам CSRF.	Лекции ЛР	10		4	1, 2	ОР 1-7
3	Поиск уязвимостей к атакам XSS.	Лекции ЛР	10		4	1, 2	ОР 1-7
4	Поиск уязвимостей к атакам SQL.	Лекции ЛР	10		4	1, 2	ОР 1-7
5	Поиск уязвимостей к атакам IDOR.	Лекции ЛР	10		4	1, 2	ОР 1-7
6	Поиск уязвимостей в механизмах управления сессиями.	Лекции ЛР	10		8	1, 2	ОР 1-7
7	Методы автоматизации поиска уязвимостей.	Лекции ЛР	10		4	1, 2	ОР 1-7
	Изучение учебного материала, подготовка к занятиям	СРС	10		68	1, 2	ОР 1-7
	Подготовка к промежуточной аттестации в форме зачета	СРС	10		6,15	1, 2	
	Прохождение промежуточной аттестации в форме зачета	Э	10		0,25		

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

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.	Л. Шкляр, Р. Розен	Архитектура веб-приложений	М.: Эксмо	2011 г., 640 с.
2.		OWASP Testing Guide	URL: https://www.owasp.org/index.php/OWASP Testing Guide v4 Table of Contents.	
Дополнительная литература				
3.	В. Кочетков	Философия Application Security	URL: https://www.youtube.com/watch?v=mb7tcT-9VXk	

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

- 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/2>.

4.3. Перечень лицензионного и программного обеспечения

Burp Suite, OWASP ZAP, VirtualBox или VMWare Player, Kali Linux

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения лабораторных занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов, проведения защиты проектов в конце семестра. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. Преподавательский состав, реализующий дисциплину

Колегов Денис Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности.

7. Язык преподавания – русский язык.