Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Научно-образовательный центр «Высшая ИТ школа»

УТВЕРЖДЕНО:
Исполнительный директор НОЦ ВИТШ

Т.С.Кетова

Рабочая программа дисциплины

Основы кибербезопасности

по направлению подготовки
09.03.04 Программная инженерия

Направленность подготовки:
«Программная инженерия»

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2022

СОГЛАСОВАНО:
Руководитель ОП
О.А.Змеев

Председатель УМК
Д.О. Змеев

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины (модуля)

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности

ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов

ОПК-7 Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой

ОПК-8 Способен осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.1 Разрабатывает алгоритмы и прототипы информационных систем для проверки теоретических, технологических или экспериментальных гипотез в процессе решения задач профессиональной деятельности

ИОПК 2.2 Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

ИОПК 3.1 Использует поисковые информационные системы, общие базы данных, в том числе библиографические базы публикаций и научных статей, с учётом основных правил оформления и использования ссылок и внешних источников

ИОПК 3.2 Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности

ИОПК 6.1 Формализует и предлагает алгоритмическое решение поставленной задачи, при условии, что задача имеет формальное и алгоритмическое решение

ИОПК 7.1 Применяет языки программирования, определения и манипулирования данными, навыки работы с базами данных, знания об операционных системах, современных программных сред разработки информационных систем для решения практических задач

ИОПК 7.2 Применяет основные концепции, принципы и факты теории доказательств для обоснования принимаемых решений в процессе практической деятельности

ИОПК 8.2 Реализует и проверяет алгоритмы или программные компоненты, осуществляющие поиск, обработку и анализ данных, с учётом требований к формату и поставленной задачи

2. Задачи освоения дисциплины

– Получить базовые знания в областях информационной и компьютерной безопасности для решения практических задач профессиональной деятельности;

– Научиться выявлять и исправлять классические уязвимости в программном коде мобильных и веб-приложений;

– Знать основные принципы, методологии и подходы безопасной разработки и развертывания программных компонент;

– Повысить общую компьютерную грамотность обучающихся.

3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Семестр 4, Зачет с оценкой.

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: “Основы математического анализа”, “Математика для компьютерных наук”, “Основы программирования”, “Языки программирования”, “Базы данных”, “Основы системного администрирования”.

6. Язык реализации

Русский

7. Объем дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

– лекции: 16.0 ч.;

– лабораторные работы: 16.0 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины (модуля), структурированное по темам

Тема 1. Введение в кибербезопасность.

Тема 2. Основы криптографии.

Тема 3. Классические веб-уязвимости.

Тема 4. Прочие программные уязвимости.

Тема 5. Введение в SSDLC.

Тема 6. Аудит информационной безопасности.

Тема 7. Код-ревью и анализ рисков.

Тема 8. Безопасное развертывание и мониторинг.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, вопросов по лекционным материалам, оценивания выполнения групповых домашних (лабораторных) работ и конрольных работы, а также фиксируется в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Дисциплина состоит из возьми групповых (командных) работ, каждая из которых

имеет теоретическую и практическую составляющую и несколько уровней сложности. Работы оцениваются по условной бальной шкале. Максимальная оценка за одну работу составляет 30 баллов. Студентам дается неделя на выполнение и защиту каждой работы.

Пример лабораторной работы:

Требуется провести код-ревью предоставленного исходного кода небольшого веб-сервиса. Каждая найденная и исправленная уязвимость оценивается в 3 балла при условии наличия подробного отчета с описанием категории уязвимости, её опасности и методики эксплуатации. Подсказка: в коде приложения не менее 10 уязвимостей и мисконфигураций.

В качестве контрольной точки между студентами проводится командное соревнование в формате “захват флага”, где обучающиеся демонстрируют навыки в поиске и исправлении уязвимостей за короткий промежуток времени. Все решенные задачи конвертируются в дополнительные баллы в соответствии с динамической шкалой: чем больше студентов решило задание, тем меньше его условная стоимость. Студенты имеют право перераспределить набранные баллы внутри команды.

Все полученные студентами баллы за лабораторные и контрольные работы суммируются и переводятся в итоговую оценку в соответствии со следующей шкалой:

Суммарный балл	Итоговая оценка	Результат аттестации
0+	2-	неудовлетворительно
20+	2	неудовлетворительно
35+	2+	неудовлетворительно
65+	3-	удовлетворительно
80+	3	удовлетворительно
110+	3+	удовлетворительно
140+	4-	хорошо
155+	4	хорошо
185+	4+	хорошо
215+	5-	отлично
230+	5	отлично
250+	5+	отлично

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине “Основы компьютерной безопасности” на платформе “Ulearn.me” - https://ulearn.me/Course/Hackerdom.

б) Оценочные материалы текущего контроля и промежуточной аттестации.

в) План лекциионных и практических занятий по дисциплине.

г) Правила дисциплины, включающие методические указания по проведению групповых лабораторных работ и организации самостоятельной работы студентов.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

- Ерохин, В. В. Безопасность информационных систем : учебное пособие : [16+] / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко ; Брянский государственный университет им. акад. И. Г. Петровского. – 4-е изд., стер. – Москва : ФЛИНТА, 2022. – 184 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562458 (дата обращения: 14.02.2023). – Библиогр. в кн. – ISBN 978-5-9765-1904-6. – Текст : электронный.
- Семь безопасных информационных технологий : учебник : [16+] / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов ; под ред. А. С. Маркова. – Москва : ДМК Пресс, 2017. – 224 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=566819 (дата обращения: 14.02.2023). – Библиогр.: с. 201 - 207. – ISBN 978-5-97060-494-6. – Текст : электронный.
- Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. – 2-е изд., стер. – Москва : ФЛИНТА, 2012. – 448 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=363419 (дата обращения: 14.02.2023). – Библиогр. в кн. – ISBN 978-5-9765-1613-7. – Текст : электронный.

б) ресурсы сети Интернет:

– Официальный сайт онлайн-сообщества с открытыми ресурсами по безопасности веб-приложений OWASP: https://owasp.org.

– Платформы для подготовки к соревнованиям в формате “Захват флага” (Capture The Flag, CTF): https://2019.hackerdom.ru, https://portswigger.net, https://play.picoctf.org, https://ctf.hacker101.com.

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ruHYPERLINK "http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system"&HYPERLINK "http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system"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/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Зоркин Александр Сергеевич,
старший системный инженер
ООО «Тинькофф Центр Разработки»

Куприянов Александр Андреевич,
ассистент учебного офиса НОЦ ВИТШ