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

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Рабочая программа дисциплины

Проектирование и разработка приложений в защищенном исполнении

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности.

ПК-1 Способен формализовать требования к программному обеспечению, спроектировать программное обеспечение, написать программный код, а также проверить работоспособность программного обеспечения и исправить дефекты.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Разрабатывает математические модели в области прикладной математики и информатики.

ИОПК-3.3 Разрабатывает и анализирует новые математические модели для решения прикладных задач профессиональной деятельности в области прикладной математики и информатики.

ИПК-1.1 Осуществляет анализ требований к программному обеспечению, построение формальной модели, проверку работоспособности программного обеспечения и исправление дефектов.

ИПК-1.2 Осуществляет разработку технических спецификаций на программные компоненты и их взаимодействие, разработку процедур проверки работоспособности и измерения характеристик программного обеспечения, разработку тестовых наборов данных.

ИПК-1.3 Осуществляет проектирование программного обеспечения, работу с системой контроля версий, рефакторинг и оптимизацию программного кода.

2. Задачи освоения дисциплины

– Освоить жизненного цикл безопасной разработки.
– Освоить практики безопасной разработки.
– Научиться применять практики безопасной разработки в жизненном цикле ПО.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в модуль «Специализация».

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

Третий семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: введение в программную инженерию, введение в компьютерную безопасность, тестирование программ, Защита информации на уровне программ и данных, алгоритмы и структуры данных, разработка программного обеспечения и скриптовые языки.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 16 ч.
-лабораторные: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Жизненный цикл разработки программного обеспечения (SDLC). Модели SDLC.

Рассматривается процесс проектирования и разработки высококачественного ПО.

Тема 2. Переход от SSDLC.

Рассматривается процесс проектирования и разработки с учетом анализа безопасности разрабатываемого ПО.

Тема 3. Перечень уязвимостей CWE, OWASP.

Знакомство с перечнем уязвимостей CWE(Common Weakness Enumeration), представляющая систему классификации недостатков безопасности, а также знакомство с OWASP(Open Web Application Security Project) – список требований к безопасности приложений и тестов, которые могут использоваться для разработки, сборки, тестирования и верификации защищённых приложений.

Тема 4. Знакомство с практиками безопасной разработки: SCA.

Рассмотрение SCA-решений с целью анализа компонентного состава и внутренних зависимостей компонентов ПО.

Тема 5. Знакомство с практиками безопасной разработки: статические анализаторы (SAST) и динамические анализаторы (DAST).

Рассмотрение SAST-решения, предназначенных для анализа исходного кода с целью обнаружения потенциальных уязвимостей на ранних этапах жизненного цикла разработки ПО. Рассмотрение DAST решения, предназначенных для обнаружения уязвимостей и слабых мест в работающем приложении.

Тема 6. Знакомство с практиками безопасной разработки: интерактивное тестирование безопасности приложений IAST.

Знакомство с решением IAST (Interactive Application Security Testing), который выполняет весь анализ в режиме реального времени.

Тема 7. Тестирование ПО.

На этапе тестирования жизненного цикла ПО внедряются дополнительные виды тестирования, такие как тестирование на проникновение, тестирование путем имитации хакерских атак, а также тестирование отказоустойчивости путём ввода случайных или заведомо неверных данных с целью вызвать сбой системы (fuzz testing).

Тема 8. Знакомство с DevSecOps.

Рассмотрение DevSecOps методологии, в частности применение лучших практик безопасности на всех этапах жизненного цикла программного обеспечения.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, выполнение лабораторных работ по курсу.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в третьем семестре проводится в письменной форме по билетам.

Билет содержит теоретический вопрос и практическую задачу. Студент письменно готовит ответ на вопросы в билете, решение практической задачи, после чего, в устной форме объясняет/защищает преподавателю подготовленный материал.

Студент допускается к экзамену в том случае, если в течение семестра успешно сдал все лабораторные работы по курсу. Продолжительность экзамена 1,5 часа

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO.

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

в) План семинарских / практических занятий по дисциплине.

г) Методические указания по проведению лабораторных работ.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– *Внуков, А. А.* Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537247 (дата обращения: 08.12.2024).

– Безопасность разработки в Agile-проектах / Л. Белл, М. Брантон-Сполл, Р. Смит, Д. Бэрд; перевод с английского А. А. Слинкин. — Москва: ДМК Пресс, 2018. — 448 с. — ISBN 978-5-97060-648-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/123703 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/414947 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

Баланов, А. Н. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 680 с. — ISBN 978-5-507-49562-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/422558 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

Гродзенский, Я. С. Информационная безопасность: учебное пособие / Я. С. Гродзенский. — Москва: Проспект, 2020. — 142 с. — ISBN 978-5-9988-0845-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/181193 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

– Блэнди, Д. Программирование на языке Rust. Быстрое и безопасное системное программирование / Д. Блэнди, Д. Орендорф; перевод с английского А. А. Слинкина. — Москва: ДМК Пресс, 2018. — 550 с. — ISBN 978-5-97060-236-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/112925 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

– Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства: учебное пособие / В. В. Бондарев. — Москва: МГТУ им. Баумана, 2017. — 228 с. — ISBN 978-5-7038-4757-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/103518 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 2-е изд. — Москва: ИНТУИТ, 2016. — 432 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/100514 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва: ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/93278 (дата обращения: 08.12.2024). — Режим доступа: для авториз. пользователей.

в) ресурсы сети Интернет:

1. Издательство «Лань» [Электронный ресурс] : электрон.-библиотечная система. – Электрон. Дан. – СПб., 2010. – URL: http://e.lanbook.com/

2. Образовательная платформа для университетов и колледжей «Юрайт». — URL: https://urait.ru/

2. ScienceDirect [Electronic resource] / Elsevier B.V. – Electronic data. – Amsterdam, Netherlands, 2016. – URL: http://www.sciencedirect.com/

3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Электрон. Дан. – М., 2000. – URL: http://elibrary/ru/defaultx.asp?

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);

– Программная среда Microsoft Visual Studio Community, интегрированная среда разработки Microsoft Visual Studio Community C++ 2017.

– Qt Creator - это кроссплатформенная интегрированная среда разработки (IDE)

– Git распределённая система управления версиями;

– GitKraken, графический кросс-платформенный клиент для работы с репозиториями и сервисами Git.

– публично доступные облачные технологии:

GitHub — крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки.

б) информационные справочные системы:

–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

– Издательство «Лань» [Электронный ресурс] : электрон.-библиотечная система. – Электрон. Дан. – СПб., 2010. – URL: http://e.lanbook.com/

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.

– Аудитории для проведения лабораторных занятий, оснащенные компьютерной техникой и доступом к сети Интернет.

– Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).

15. Информация о разработчиках

Андреева Валентина Валерьевна, к.т.н., доцент, доцент кафедры компьютерной безопасности, ИПМКН.