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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Руководитель ОПОП

_____ В.Н. Тренькаев

« 22 » мая 2025 г.

Рабочая программа учебной практики

Учебно-лабораторный практикум; Защита программ и данных

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
«Анализ безопасности компьютерных систем»

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

Код дисциплины в учебном плане: Б.2.О.01.01 (У)

СОГЛАСОВАНО:
Председатель УМК

_____ С.П. Сущенко

Томск – 2025

1. Цель практики

Целью учебной практики является закрепление и углубление подготовки специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий.

2. Задачи практики

– применение полученных знаний при осуществлении теоретических и экспериментальных научно-исследовательских работ по оценке защищенности информации в компьютерных системах;

– научиться проводить аттестацию технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты;

– научиться проводить установку, наладку, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем.

3. Место практики в структуре образовательной программы

Практика относится к обязательной части образовательной программы.

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

Семестр 9, зачет.

5. Входные требования для освоения практики

Для успешного освоения практики требуются результаты обучения по следующим дисциплинам: Языки программирования, Операционные системы.

6. Способы и формы проведения практики

Практика проводится на базе ТГУ. Способы проведения: стационарная.

7. Объем и продолжительность практики

Объем практики составляет 2 зачётных единицы, 72 часа.

8. Планируемые результаты практики

Результатами прохождения практики являются следующие индикаторы достижения компетенций:

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных

ИОПК-9.3 Обладает знанием и демонстрирует навыки применения методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

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.

ИОПК-14.1 Понимает модели и структуры данных, физические модели баз данных, принципы организации и методы проектирования баз данных, языки и системы программирования баз данных

ИОПК-14.2 Производит обеспечение и оптимизацию функционирования систем управления базами данных, а также предотвращение потерь и повреждений данных в них

ИОПК-14.3 Оценивает состояние и эффективность системы безопасности на уровне базы данных, разворачивает и настраивает средства защиты базы данных от несанкционированного доступа

ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности

ИОПК-18.2 Оценивает соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам

ИОПК-18.3 Составляет и оформляет аналитический отчет по результатам проведенного анализа, разрабатывает предложения по устранению выявленных уязвимостей

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

ИОПК-19.3 Осуществляет сбор и анализ полученных результатов проверки работоспособности программного обеспечения, оценку соответствия программного обеспечения требуемым характеристикам

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.

ИПК-1.1 Проводит анализ возможностей реализации требований к программному обеспечению.

ИПК-1.2 Проводит оценку времени и трудоемкости реализации требований к программному обеспечению.

ИПК-1.3 Осуществляет согласование требований к программному обеспечению с заинтересованными сторонами.

ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации.

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.

9. Содержание практики

Практика проходит в форме выполнения лабораторных работ, направленных на формирование требуемых компетенций.

Обязанности обучающегося: ознакомиться с заданием на практику, подчиняться действующим в организации правилам внутреннего трудового распорядка; строго соблюдать правила, касающиеся техники безопасности, порядка использования предоставленного оборудования и имущества; выполнять указания руководителя практики; нести персональную ответственность за сохранность и конфиденциальность предоставленной информации; обеспечить высокое качество выполняемых работ, согласовывать свои действия с руководителем практики; вести записи в дневнике практики, отражая объем выполнения работ, особенности, возникшие трудности, выводы, предложения, замечания и т.д.; в установленный срок подготовить и представить на кафедру отчет о практике.

№ п/п	Разделы (этапы) практики, содержание	Количество часов			Формы текущего контроля
		Контактная работа	СРС	Всего	
1	Анализ программных реализаций	10	6	16	Лабораторная работа
2	Защита программ от изучения	10	6	16	Лабораторная работа
3	Программные закладки	4	6	10	Лабораторная работа
4	Внедрение программных закладок	4	6	10	Лабораторная работа
5	Противодействие программным закладкам	4	6	10	Лабораторная работа
	Сдача промежуточной аттестации в форме зачета	1,85	8,15	10	Зачет
	Итого	33,85	38,15	72	

10. Формы отчетности по практике

По итогам прохождения практики обучающиеся в срок до завершения периода практики по календарному графику предоставляют руководителю практики от ТГУ: дневник практики, отчет по практике (отчеты по лабораторным работам).

11. Организация промежуточной аттестации обучающихся

11.1 Порядок и форма проведения промежуточной аттестации

В конце 9 семестра промежуточная аттестация проводится в форме зачета. Зачет осуществляется в виде защиты лабораторных работ и ответов на теоретические вопросы.

11.1.1 Отметка «Зачтено» выставляется, если:

студент выполнил лабораторные работы и владеет большей частью теоретического материала.

11.1.2 Отметка «Не зачтено» выставляется, если:

– студент не выполнил лабораторные работы и/или не освоил большую часть теоретического материала.

12. Перечень рекомендованной литературы и ресурсов сети Интернет

а) основная литература:

– Защита программ и данных, Учебное пособие, Проскурин, В. Г., 2011

– Программирование на языке ассемблера NASM для ОС Unix, Учебное пособие, Столяров А.В., 2011

б) дополнительная литература:

– Reverse Engineering для начинающих, Юричев, Д., Электронный ресурс https://beginners.re/main.html

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Oracle VM VirtualBox / VMware Workstation Player или аналогичная система виртуализации.

– Дизассемблер IDA Freeware, Binary Ninja или аналогичный

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

– 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-техническая база проведения практики

Аудитории для проведения лабораторных занятий, индивидуальных и групповых консультаций, самостоятельной работы, текущего контроля и промежуточной аттестации, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент кафедры компьютерной безопасности.