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_» _июля_ 2021 г.

Защита в операционных системах

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	*4 з.е.*
Часов по учебному плану	*144*
в том числе:	
аудиторная контактная работа	*52.65*
самостоятельная работа	*91.35*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр А – зачет с оценкой*

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 «Защита в операционных системах» 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 – теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий построения защищенных ОС, а также средств и методов обеспечения защиты информации в ОС.

1. Место дисциплины в структуре ОПОП

Дисциплина «Защита в операционных системах» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: Языки программирования, Операционные системы, Криптографические методы защиты информации

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-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-9.1 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.	ОР-1 Знать средства и методы хранения и передачи аутентификационной информации. ОР- 2 Знать защитные механизмы и средства обеспечения безопасности операционных систем.
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях.	ОР-3 Знать требования к подсистеме аудита и политике аудита. ОР-4 Уметь формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. ОР-5 Уметь осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.
ОПК-18. Способен проводить анализ защищенности и осуществлять поиск уязвимости	ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя	ОР-6 Владеть навыками оценки уровня защиты операционных систем. ОР-7 Владеть навыками разработки программных модулей, реализующих задачи,

компьютерной системы.	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.	связанные с обеспечением безопасности операционных систем.

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	Семестр А	всего
Общая трудоемкость	144	144
Контактная работа:	52,65	52,65
Лекции (Л):		
Практики (ПЗ)	32	32
Лабораторные работы (ЛР)	16	16
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	2,4	2,4
Промежуточная аттестация	0,25	0,25
Самостоятельная работа обучающегося:	57,6	57,6
- подготовка к лабораторным и практическим занятиям	23,85	23,85
Подготовка к рубежному контролю по теме/разделу	33,75	33,75
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Зачет с оценкой**	**Зачет с оценкой**

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 защищенной операционной системы	Практики, ЛР	10		2	1, 2	ОР 1-7
2.	Управление доступом	Практики, ЛР	10		12	1, 2	ОР 1-7
3.	Идентификация, аутентификация и авторизация	Практики, ЛР	10		12	1, 2	ОР 1-7
4.	Аудит	Практики, ЛР	10		12	1, 2	ОР 1-7
5.	Интеграция защищенных операционных систем в защищенную сеть	Практики, ЛР	10		10	1, 2	ОР 1-7
	Подготовка к промежуточной аттестации в форме зачета с оценкой	СРС	10		**2,4**	**1, 2**	
	Прохождение промежуточной аттестации в форме зачета с оценкой	Э	10		**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.	Бэндл Дэвид	Защита и безопасность в сетях Linux	Питер	2002, 480с
2.	Проскурин В.Г.	Защита в операционных система. Учебное пособие	Горячая линия Телеком	2019, 192с
Дополнительная литература				
4.	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие.	Горячая линия Телеком	2016, 320с
5.	Furgel, I., & Saftig, V.	Common Criteria Protection Profile “Multiple Independent Levels Of Security: Operating System”	EURO-MILS	2016, 61с
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

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.

5. Методические указания обучающимся по освоению дисциплины

Обучающимся необходимо на лекциях строго фиксировать содержание излагаемого материала, перед каждой следующей лекцией освежать содержание предыдущей (при необходимости – предыдущих) лекции. В случае трудностей восприятия содержания – готовить вопросы преподавателю к очередной лекции.

6. Преподавательский состав, реализующий дисциплину

Брославский Олег Викторович, ассистент кафедры компьютерной безопасности ТГУ.

7. Язык преподавания – русский язык.