Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Защита в операционных системах

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель: Шавыкин О.В.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью освоения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий построения защищенных операционных систем, а также средств и методов обеспечения защиты информации в операционных системах.

Задачами освоения дисциплины являются:

- изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности операционных систем;
- изучение средств и методов управления доступом в защищенных операционных системах;
- изучение средств и методов аутентификации пользователей в защищенных операционных системах;
- изучение средств и методов реализации аудита в защищенных операционных системах;
- изучение средств и методов интеграции защищенных операционных систем в защищенную сеть.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Методы программирования», «Операционные системы», «Основы информационной безопасности».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Основы построения защищенных компьютерных сетей», «Технология разработки информационных систем в защищенном исполнении», «Сети и системы передачи информации».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

практические занятия – 17 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 57 часа.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**ОПК-8.3** Использует защитные механизмы и средства обеспечения безопасности операционных систем

ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	**ОПК-11.2** Настраивает политику безопасности основных операционных систем
ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	**ОПК-12.1** Применяет основные принципы конфигурирования и администрирования операционных систем
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	**ОПК-13.1** Проектирует программные модули, реализующие задачи, связанные с обеспечением безопасности операционных систем распространенных семейств

5. Форма промежуточной аттестации и семестр прохождения – зачет в 7 семестре.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
Раздел 1. Построение защищенных операционных систем.		2	1	0	4
Раздел 2. Формальные модели управления доступом		2	1	0	4

Раздел 3. Идентификация, аутентификация и авторизация		2	1	0	4
Раздел 4. Защащищенная операционная система Astra Linux Special Edition: архитектура и режимы функционирования средств защиты информации		2	1	0	4
Раздел 5. Мандатный контроль целостности		2	1	0	4
Раздел 6. Мандатное управлением доступом		2	1	0	4
Раздел 7. Защищенная работа с файлами		2	1	0	3
Раздел 8. Аудит защищенной системы		2	1	0	3
Раздел 9. Реализация замкнутой программной среды		2	1	0	3
Раздел 10. Режим киоска		2	1	0	3
Раздел 11. Интеграция защищенных операционных систем в защищенную сеть		2	1	0	3
Раздел 12. Служба Astra Linux Directory (ALD)		2	1	0	3
Раздел 13. Мандатное управление доступом в СУБД PostgreSQL		2	1	0	3
Раздел 14. Дополнительные функции безопасности системы		2	1	0	3
Раздел 15. Red Book: настройка безопасной конфигурации для Astra Linux Special Edition		2	1	0	3
Раздел 16. Системы обнаружения/предотвращения вторжений		2	1	0	3

Раздел 17. Нормативные документы ФСТЭК России, регламентирующие требования безопасности информации		2	1	0	3
ИТОГО	108	34	17	0	57

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1. Построение защищенных операционных систем.	лабораторная работа лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
Раздел 2. Формальные модели управления доступом		Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления
Раздел 3. Идентификация, аутентификация и авторизация		
Раздел 4. Защащищенная операционная система Astra Linux Special Edition: архитектура и режимы функционирования средств защиты информации		
Раздел 5. Мандатный контроль целостности		Дискуссионные технологии, кейс-технология, методы группового решения творческих задач.
Раздел 6. Мандатное управлением доступом		
Раздел 7. Защищенная работа с файлами		
Раздел 8. Аудит защищенной системы		
Раздел 9. Реализация замкнутой программной среды		
Раздел 10. Режим киоска		
Раздел 11. Интеграция защищенных операционных систем в защищенную сеть		
Раздел 12. Служба Astra Linux Directory (ALD)		

Раздел 13. Мандатное управление доступом в СУБД PostgreSQL	лабораторная работа лекция	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления
Раздел 14. Дополнительные функции безопасности системы		
Раздел 15. Red Book: настройка безопасной конфигурации для Astra Linux Special Edition		
Раздел 16. Системы обнаружения/предотвращения вторжений		
Раздел 17. Нормативные документы ФСТЭК России, регламентирующие требования безопасности информации		

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (ОПК-8.3; ОПК-11.2; ОПК-12.1): Перечислите основные этапы построения защиты операционной системы.

Задание 2 (ОПК-8.3; ОПК-11.2; ОПК-12.1): Что значит фраза «процесс А имеет более низкий приоритет чем Б»?

Раздел II.

Задание 1 (ОПК-11.2; ОПК-12.1): Пусть в некоторой системе, построенной на основе модели мандатного ролевого управления доступом, субъект с высоким текущим уровнем доступа может назначать любые права доступа к сущности некоторой роли, доступной в качестве текущей субъекту с низким уровнем доступа. Постройте пример реализации информационного потока по времени от сущности с высоким уровнем конфиденциальности к сущности с низким уровнем конфиденциальности с использованием прав доступа такой роли.

Раздел III.

Задание 1 (ОПК-8.3; ОПК-11.2): *Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard». Составить программу, которая записывает пароль следующим образом*:

1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом первого слова на экране; если это буква «z», записать «a».

2. В качестве второго символа записать букву, которая в алфавите предшествует предпоследней букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».

3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся предшественником среднего символа третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».

4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах плюс 1 символ; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.

Дополнить полученную программу средствами аутентификации:

1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».

2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.

3. Вывести результат аутентификации: пароль верен или неверен?

Раздел IV.

Задание 1 (ОПК-11.2; ОПК-12.1): Администратор системы неоднократно сообщал о действиях в системе, выполняемых кем-то под его учетной записью, включая смену паролей пользователей. Администратор безопасности посчитал необходимым настроить полный аудит ветви реестра, хранящий учетные записи и их пароли в неявном виде. Ветвь реестра, хранящая базу данных учетных записей, имеет следующий путь: «PASSWORD_LOCAL_PC\MMM\MMM». Выясните, кто и какой программой получает доступ к базе данных учетных записей.

Раздел V.

Задание 1 (ОПК-8.3; ОПК-13.1): Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Windows, функционирующей в составе локальной вычислительной сети, построенной на основе "лесной" доменной архитектуры и физически изолированной от глобальных вычислительных сетей общего пользования.

Задание 2 (ОПК-8.3; ОПК-13.1): Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Linux.

Задание 3 (ОПК-8.3; ОПК-13.1): Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Windows CE для платформы карманных портативных компьютеров и смартфонов.

Оценочные материалы для проведения промежуточной аттестации

Проверяемые индикаторы достижения компетенций: ОПК-8.3; ОПК-11.2; ОПК-12.1; ОПК-13.1

Каждый студент отвечает на вопросы теста и дает развернутый ответ на теоретический вопрос.

Примерные вопросы к зачету

1. Субъекты, объекты, методы, права и привилегии Linux.
2. Субъекты, объекты, методы, права и привилегии Windows.
3. Дискреционное управление доступом в современных операционных системах.
4. Средства защиты от вредоносного программного обеспечения в современных операционных системах.
5. Проблемы реализации мандатного управления доступом в современных операционных системах.
6. Управление доступом в UNIX.
7. Базовые средства управления доступом в Windows: маркеры доступа, дескрипторы защиты.
8. Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты.
9. Управление средствами аутентификации в Linux.
10. Управление доменами Windows.
11. Какова роль аудита в обеспечении безопасности компьютерной системы?
12. Где и каким образом формируется информация о событиях аудита?
13. Какая информация может быть получена в результате аудита?
14. Какие типы аудита вы знаете и для чего предназначен каждый из них?
15. Каким образом активизируется политика аудита?
16.. Каким образом политика аудита применяется для выбранных объектов и пользователей?
17. В каких случаях целесообразно учитывать *Успех,* а когда целесообразно фиксировать *Отказ?*
18. Как пользоваться журналами безопасности?
19. Какие учетные записи дают право на настройку аудита и проверку результатов аудита? Каким образом администратор может использовать информацию об аудите для повышения безопасности системы?

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения зачета необходимо ответить на вопросы теста и дать ответ на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется решение теста верное от 85 – 100% всех заданий.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Верно даны ответы на 70-84% тестовых заданий.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Правильные решения тестовых заданий составляют от 41-69%.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Правильные тестовые ответы составляют менее 40%.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин; Московский институт электронной техники. - 1. - Москва : Издательский Дом "ФОРУМ", 2023. - 416 с. – Режим доступа : https://znanium.com/catalog/document?id=418929.

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю. Н. Сычев; Российский экономический университет им. Г.В. Плеханова. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 201 с. - (Высшее образование: Магистратура). - ВО - Бакалавриат. –Режим доступа: https://znanium.com/catalog/document?id=420080

Сергеева, Ю.С. Защита информации: Конспект лекций: учебное пособие / Ю.С. Сергеева. - М. : А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=72670

б) Дополнительная литература:

Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург : Лань, 2023. - 124 с. - Книга из коллекции Лань - Информатика. – Режим доступа: https://e.lanbook.com/book/293009

Вержаковская М. А. Вычислительные системы, операционные системы, сетевые технологии и информационные ресурсы [Электронный ресурс] : учебное пособие / М. А. Вержаковская, В. Ю. Аронов. - Самара : ПГУТИ, 2022. - 181 с. – Режим доступа: https://e.lanbook.com/book/320834M.

Кудрявцев Н. Г. Основы работы в ОС Linux. Начальное конфигурирование и администрирование [Электронный ресурс] : учебное пособие / Н. Г. Кудрявцев, И. Н. Фролов. - Горно-Алтайск : ГАГУ, 2022. - 108 с. – Ht;bv ljcnegf: https://e.lanbook.com/book/271097

2) Программное обеспечение

Adobe Acrobat Reader DC - Russian	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Git version 2.5.2.2	бесплатно
Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022

Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011;
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012;
Многофункциональный редактор ONLYOFFICE	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
MySQL Workbench 6.3 CE	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;
PostgreSQL 9.6	бесплатно
Python 3.4.3	бесплатно
Visual Studio 2010 Prerequisites - English	Акт на передачу прав №785 от 06.08.2021 г.
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
WinPcap 4.1.3	бесплатно
Wireshark 2.0.0 (64-bit)	бесплатно
R studio	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.

2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.

3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.

4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.

5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозитарий ТвГУ http://eprints.tversu.ru

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
www.fstec.ru Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	50	18	12	20
2	50	18	12	20

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:
https://tversu.ru/sveden/files/204-R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория № 314 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Мультимедийный комплект учебного класса	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice –бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО-бесплатно
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, у*чебная аудитория* 203, 224, 170002, г.Тверь, Садовый пер-к, д. 35	Столы, стулья, переносной ноутбук, проектор	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice –бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО-бесплатно

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Реквизиты документа, утвердившего изменения
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
2.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016

3.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
4.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2017
5.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
6.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023