Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП:
_____ Н.А. Семыкина
«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ

специальность 10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Уровень высшего образования
СПЕЦИАЛИТЕТ

Для студентов 4курса очной формы обучения

Составитель:
к.ф.-м.н., доцент _____ Н.А. Семыкина

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Защита в операционных системах

2. Цель и задачи дисциплины (или модуля)

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.

Задачи дисциплины:

- 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.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина «Защита в операционных системах» относится к дисциплинам базовой части. Для успешного изучения данной дисциплины необходимо знание основ следующих дисциплин «Информатика», «Аппаратные средства вычислительной техники», «Операционные системы». Дисциплина «Защита в операционных системах» является предшествующей для следующих базовых дисциплин: «Основы построения защищенных баз данных», «Техническая защита информации». Знания и практические навыки, полученные в результате изучении дисциплины «Защита в операционных

системах», используются студентами при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):

4 зачетные единицы, 144 академических часа, **в том числе**

контактная работа: лекции 30 часов, практические занятия 30 часов, **самостоятельная работа:** 21 час, **контроль**: 63 часа.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (или модулю)**
ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** навыками поиска и обработки информации по профилю деятельности. **Уметь:** использовать международные и отечественные стандарты. **Знать:** основные понятия, функции, состав и принципы работы операционных систем.
ПК-8. способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	**Владеть:** навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств. **Уметь:** формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. **Знать:** средства и методы хранения и передачи аутентификационной информации; защитные механизмы и средства обеспечения

	безопасности операционных систем
ПК-11. Способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	**Владеть:** методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. **Уметь:** производить тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности компьютерных систем. **Знать:** требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем.

6. Форма промежуточной аттестации - экзамен.

7. Язык преподавания русский**.**

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

Учебная программа – наименование разделов	Всего (час.)	Контактная работа (час.)		Самостоятельная работа (час.)	Контроль (час.)
		Лекции	Практические (лабораторные) занятия		
Раздел 1. Понятие защищенной операционной системы	28	6	6	4	12
Раздел 2. Управление доступом	34	7	7	5	15
Раздел 3. Идентификация, аутентификация и авторизация	32	7	7	4	14

Раздел 4. Аудит защищенной системы	22	4	4	4	10
Раздел 5. Интеграция защищенных операционных систем в защищенную сеть	28	6	6	4	12
ИТОГО	144	30	30	21	63

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические рекомендации по организации самостоятельной работы студентов

Самостоятельная работа студентов по изучаемой дисциплине призвана, не только, закреплять знания, полученные во время аудиторных занятий, но и способствовать развитию у студентов творческих навыков, инициативы, умению организовывать свое время.

Все виды самостоятельной работы и планируемые на их выполнение затраты времени в часах исходят из того, что студент достаточно активно работал в аудитории, слушая лекции и решая задачи на практических занятиях. В случае пропуска лекций и практических занятий студенту потребуется сверхнормативное время на освоение пропущенного материала.

При выполнении плана самостоятельной работы студенту необходимо прочитать теоретический материал, содержащийся в указанной учебной литературе и Интернет-ресурсах. Составить словарь основных терминов и тематические конспекты, в которые необходимо включить теоретическое описание метода и привести примеры алгоритмов.

Раздел 1. Понятие защищенной операционной системы

Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной

системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.

Раздел 2. Управление доступом

Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах.

Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в SCO UNIX, Solaris, Linux.

Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа, привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам. Средства динамического изменения полномочий субъектов: олицетворение субъектов доступа. Расширения дискреционной системы управления доступом: автоматическое наследование атрибутов защиты объектов, ограниченные маркеры доступа, мандатный контроль целостности, контроль учетных записей, элементы изолированной программной среды.

Раздел 3. Идентификация, аутентификация и авторизация

Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей.

Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в UNIX, библиотеки PAM. Парольная аутентификация в Windows, средства управления параметрами аутентификации.

Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей.

Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.

Раздел 4. Аудит защищенной системы

Необходимость аудита в защищенной системе. Требования к подсистеме аудита. Реализация аудита в UNIX и Windows.

Раздел 5. Интеграция защищенных операционных систем в защищенную сеть

Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Сквозная аутентификация, возникающие проблемы и способы их решения. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене.

«Лесная» доменная архитектура Windows, ее преимущества по сравнению с «плоской» доменной архитектурой Windows NT. Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Средства и методы синхронизации баз данных контроллеров разных доменов одного леса. Аутентификация по Kerberos. Групповая политика. Делегирование полномочий.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

Типовые контрольные задания для проверки уровня сформированности компетенций ОПК-3, ПК – 8, 11.

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый, **Владеть**	1. Что значит фраза «процесс А имеет более низкий приоритет чем Б»? a) численное значение приоритета А больше чем значение приоритета Б b) численное значение приоритета А меньше чем значение приоритета Б c) процесс А получит при планировании меньше	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение

	ресурсов чем процесс Б + d) процесс А выполняется визуально быстрее чем Б e) процессу А выделяется кванты большего размера чем Б f) процесс будет быстрее занимать свободную память 2. Разграничение доступа к ресурсам: A. порядок использования ресурсов автоматизированной системы, при котором осуществляется ограничение доступа субъектов к объектам системы B. порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами C. порядок использования ресурсов автоматизированной системы, при котором объекты получают доступ к субъектам системы в строгом соответствии с установленными правилами. D. порядок использования ресурсов автоматизированной системы, при котором осуществляется ограничение доступа к ресурсам системы	– 0 баллов

Базовый, **Уметь**	1.Слабости парольной защиты: 1. трудность распознавания 2. возможность раскрытия пароля путем подбора 3. возможность обхода парольной защиты 2. В асимметричных системах шифрования: 1. ключ шифрования совпадает с ключом расшифрования 2. ключ шифрования отличается от ключа расшифрования 3. ключи генерируются случайным образом	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов
Базовый, **Знать**	1. Заражение компьютерными вирусами может произойти в процессе ... A) работы с файлами B) форматирования дискеты C) выключения компьютера D) печати на принтере E) правильных ответов нет. 2. Какие программы не относятся к антивирусным? A) программы-фаги B) программы сканирования C) программы-ревизоры D) прогаммы-детекторы E) правильных ответов нет. 3. Какого вида аутентификации в ОС не существует: A) По знаниям	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов

	B) По собственности C) По паспорту субъекта D) По биометрическим параметрам	

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

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

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

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

VII. Методические указания для обучающихся по освоению дисциплины

Требования к рейтинг-контролю

Модуль 1.

Максимальная сумма баллов по модулю – 30, из них 15 баллов отводится на текущий контроль учебной работы студента, 15 баллов на рубежный контроль по модулю.

Текущая работа студента складывается из ответов в аудитории и подготовке сообщений, min – 0 баллов, max - 3 баллов.

Рубежный контроль проводится в форме контрольной работы.

Модуль 2.

Максимальная сумма баллов по модулю – 30, из них 15 баллов отводится на текущий контроль учебной работы студента, 15 баллов на рубежный контроль по модулю.

Текущая работа студента складывается из ответов в аудитории и подготовке сообщений, min – 0 баллов, max - 3 баллов.

Рубежный контроль проводится в форме контрольной работы.

Примерный перечень тем домашних заданий:

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.
2. Разработать спецификации задания по безопасности для подсистемы аудита операционной системы Windows.
3. Разработать спецификации задания по безопасности для подсистемы аутентификации пользователей операционной системы Windows.
4. Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Linux.
5. Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Windows CE для платформы карманных портативных компьютеров и смартфонов.

Примерный перечень вопросов для контрольной работы:

1. Субъекты, объекты, методы, права и привилегии Linux и Windows.
2. Дискреционное управление доступом в современных операционных системах.
3. Средства защиты от вредоносного программного обеспечения в современных операционных системах.
4. Проблемы реализации мандатного управления доступом в современных операционных системах.

Примерный перечень вопросов для опросов на практических занятиях:

1. Управление доступом в UNIX.
2. Базовые средства управления доступом в Windows: маркеры доступа, дескрипторы защиты.
3. Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты.
4. Управление средствами аутентификации в Linux.
5. Управление доменами Windows.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по

дисциплине (или модулю), включая перечень программного обеспечения и информационных справочных систем (по необходимости)

1) лекционные занятия в аудитории, с использованием мультимедийной установки;
2) практические занятия с использованием средств мультимедиа.

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски.

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

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№ п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	Вся рабочая программа	Приведена в соответствие с новым стандартом и новым шаблоном	
2.			