ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

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

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК - 1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК - 12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

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.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-1.1. Использует современные достижения отечественной и зарубежной науки и техники в области информационных технологий и информационной безопасности	**Знает** принципы построения подсистем защиты в операционных системах **Умеет** пользоваться средствами защиты, предоставляемыми операционной системой
ОПК-12.1. Использует теоретические основы построения баз данных, модели данных, принципы организации вычислительных сетей, сетевые технологии, технические средства их реализации, организации и виды операционных систем	**Знает** основные приемы настройки подсистем информационной безопасности операционных систем **Умеет** планировать политику безопасности операционной системы, применять на практике методы и инструментарий конфигурирования и настройки средств защиты информации в операционных системах

3. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность операционных систем» относится к обязательной части, образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация - **Анализ безопасности информационных систем.**

4. Структура и содержание

Дисциплина «Безопасность операционных систем» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 144 академических часов (4 зачетных единицы).

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			6
Общая трудоемкость дисциплины по учебному плану	**4**	**144**	**144**
Контактная работа, в том числе:		**56**	**56**
Аудиторные занятия		**54**	**54**
Лекции (Л)		16	16
Практические занятия (ПЗ)		38	38
Консультация		**2**	2
Самостоятельная работа (СРС)		**52**	**52**
Экзамен		**36**	36

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов и тем	**Всего часов**	**Количество часов по видам занятий**				**Самостоятельная работа**
		Лекции	**Практические занятия**	**Консультации**	**Контроль**	
6 семестр						
Понятие защищенной операционной системы	24	4	8			12
Управление доступом	26	4	10			12
Идентификация, аутентификация и авторизация	28	4	10			14
Интеграция защищенных операционных систем в защищенную сеть	28	4	10			14
Консультация	2			2		
Экзамен	36				36	
итого за 6 семестр	**144**	**16**	**38**	**2**	**36**	**52**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Понятие защищенной операционной системы

Лекции. Общая характеристика ОС; назначение и возможности систем семейства UNIX, систем семейства Windows. Интерфейс взаимодействия ОС с

пользователями. Общие принципы управления ресурсами вычислительных систем. Понятия процесса (потока) в ОС.

Практические занятия. Средства межпроцессорного взаимодействия. Управление памятью в ОС. Виртуальная память. Обработка прерываний от устройств ввода-вывода в ОС. Структурная обработка исключений. Синхронный и асинхронный ввод-вывод. Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной системы.

Самостоятельная работа. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.

Рекомендуемая литература:

основная [1, 2];

дополнительная [1,2]

Раздел 2. Управление доступом

Лекции. 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.

Практические занятия. Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полно- мочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в 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.

Самостоятельная работа. Расширения дискреционной системы управления доступом: автоматическое наследование атрибутов защиты объектов, ограниченные маркеры доступа, мандатный контроль целостности, контроль учетных записей, элементы изолированной программной среды.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2]

Раздел 3. Идентификация, аутентификация и авторизация

Лекции. 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.

Практические занятия. Парольная аутентификация в Linux, 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.

Самостоятельная работа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2]

Раздел 4. Интеграция защищенных операционных систем в защищенную сеть

Лекции. Преимущества доменной архитектуры локальной сети. Понятие домена,

контроллер домена. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене.

Практические занятия. «Лесная» доменная архитектура Windows 2000/2003/2008/2010. Идентификация компьютеров в сети. Двусторонние транзитивные отношения

доверия. Средства и методы синхронизации баз данных контроллеров

разных доменов одного леса. Аутентификация по Kerberos.

Самостоятельная работа. Групповая политика. Делегирование полномочий.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2]

5. Методические рекомендации по организации изучения дисциплины «Безопасность операционных систем»

При реализации программы дисциплины используются лекционные и практические занятия.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники;

– концентрировать внимание обучающихся на наиболее сложных и узловых вопросах;

– стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цели практического занятия: выработка практических умений и приобретение навыков, закрепление пройденного материала по соответствующей теме дисциплины.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине «Безопасность операционных систем»

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме опроса и тестирования.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме экзамена в 6 семестре.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса:

- Определение и назначение ОС
- Виды ОС
- Функции ОС
- Архитектура операционной системы
- Структура ОС

– Монолитная архитектура
– Микроядерная архитектура
– Понятия вычислительного процесса и ресурса
– Прерывания
– Системные вызовы
– Процесс, поток
– Создание процессов и потоков
– Состояния потока
– Планирование и диспетчеризация потоков
– Алгоритмы планирования
– Управление памятью
– Типы адресов
– Методы распределения памяти без использования дискового пространства
– Методы распределения памяти с использованием дискового пространств

Примерный перечень вопросов выносимых на экзамен

1. Понятие виртуальной памяти
2. Страничное распределение виртуальной памяти
3. Сегментное распределение виртуальной памяти
4. Странично-сегментное распределение виртуальной памяти
5. Свопинг
6. Назначение и функции файловой системы
7. Логическая организация файловой системы
8. Файловая система FAT
9. Файловая система NTFS
10. Контроль доступа к файлам
11. Основные понятия безопасности ОС
12. Системный подход к обеспечению безопасности
13. Симметричные криптосистемы
14. Асимметричные криптосистемы
15. Аутентификация
16. Аутентификация на основе многоразовых паролей
17. Аутентификация на основе одноразовых паролей
18. Цифровые сертификаты
19. Цифровые подписи
20. Авторизация доступа
21. Аудит
22. Средства администрирования ОС Windows Server
23. Средства безопасности ОС Windows Server
24. Планирование и диспетчеризация потоков

25. Алгоритмы планирования
26. Управление памятью
27. Управление доступом в Linux
28. Управление доступом в Windows
29. Анализ операционных систем
30. Средства аутентификации операционных систем
31. Управление средствами аутентификации в Linux
32. Управление средствами аутентификации в Windows
33. Документирование политики безопасности
34. Централизованное планирование политики безопасности в лесу доменов Windows
35. Централизованное планирование политики безопасности в Linux

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
экзамен	правильность и полнота ответа; выполнение контрольных нормативов	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя.	хорошо
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	удовлетворительно
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	неудовлетворительно

7. Ресурсное обеспечение дисциплины «Безопасность операционных систем»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- Статистическая диалоговая система STADIA [ПО-6FF-561] - Статистическая диалоговая система [Лицензионное. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 9064]

- SMath Studio [ПО-A68-516] - Программное обеспечение для вычисления математических выражений и построения графиков функций [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 12849]

- МойОфис Образование [ПО-41B-124] - Полный комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4557]

- Astra Linux Common Edition релиз Орел [ПО-25B-603] - Операционная система общего назначения "Astra Linux Common Edition" [Коммерческая (Full Package Product). Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4433]

7.2. Профессиональные базы данных и информационные справочные системы

1. Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс]. – Режим доступа: http://window.edu.ru/, доступ только после самостоятельной регистрации
2. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации
3. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ
4. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный доступ

7.3. Литература

Основная литература:

1. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие для вузов / В. Г. Кобылянский. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 120 с. — ISBN 978-5-507-44969-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/254651 (дата обращения: 31.08.2023). — Режим доступа: для авториз. пользователей.

2. Киренберг, Информационная безопасность современных операционных систем : учебное пособие / Киренберг, Г. А. . — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/295736 (дата обращения: 31.08.2023). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Филиппов А.А. Операционные системы: учебное пособие / Филиппов А.А.. — Ульяновск: Ульяновский государственный технический университет, 2021. — 100 с. — ISBN 978-5-9795-2129-9. — Текст: электронный // IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/121273.html

2. Олифер В., Олифер Н. Компьютерные сети. Принципы технологии протоколы. Юбилейное издание. Учебник – издательство «Питер», 2021. – 1008 с.

3. Платунова, С. М. Администрирование вычислительных сетей на базе MS Windows Server® 2008 R2 : учебное пособие — СПб. : Университет ИТМО, 2013. — 127 с. — Режим доступа: http://www.iprbookshop.ru/68640.html

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Авторы: к.т.н., доцент Максимов А.В.