МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Безопасность операционных систем»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Доцент, к.ф.-м.н. Д.В.Ильин

старший преподаватель С.О. Иванов

ОБСУЖДЕНО:

на заседании кафедры математического и аппаратного обеспечения информационных систем «30» августа 2017г., протокол №1

заведующий кафедрой Д.В. Ильин

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники «30» августа 2017г., протокол №1

Декан факультета А.В. Щипцова

Директор научной библиотеки Н.Д. Никитина

Начальник управления информатизации И.П. Пивоваров

Начальник учебно-методического управления В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Целью изучения дисциплины «Безопасность операционных систем» является подготовка обучаемых к эксплуатации современных операционных систем (ОС) в соответствии с требованиями информационной безопасности с учетом особенностей их устройства.

Основными задачами дисциплины являются:

- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Безопасность операционных систем» относится к числу дисциплин базовой части. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Основы информационной безопасности».

Дисциплина является предшествующей для дисциплин: «Безопасность сетей ЭВМ», «Управление информационной безопасностью», «Организация ЭВМ и вычислительных систем», прохождения практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

– способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

– способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

– способность управлять информационной безопасностью автоматизированной системы (ПК-28).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

– принципы построения и функционирования современных операционных систем (З1);

– принципы организации и структуру подсистем защиты операционной системы (З2);

– принципы работы подсистемы информационной безопасности операционных систем (З3);

– методы управления информационной безопасностью операционной системы (З4);

уметь:

– оценивать эффективность и надёжность компонентов операционной системы (У1);

– настраивать компоненты операционной системы для выполнения требований информационной безопасности (У2);

– использовать средства защиты операционных систем (У3);

– уметь использовать средства контроля информационной безопасности операционных систем (У4);

владеть навыками:

– настройки информационных процессов операционной системы (Н1);
– настройки эффективной и безопасной работы операционной системы (Н2);
– установки и настройки средств защиты операционной системы (Н3);
– управления подсистемой информационной безопасности операционных систем (Н4).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);
– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Организация операционных систем.	ОПК-8, ПК-24	З1,2, Н1, Н2, У1, У2
Тема 1.1. Операционные системы.		
Тема 1.2. Управление задачами.		
Тема 1.3. Управление памятью.		
Тема 1.4. Управление устройствами хранения данных.		
Тема 1.5. Управление внешними устройствами.		
Тема 1.6. Управление связью.		
Тема 1.7. Управление функциональностью.		
Раздел 2. Средства защиты операционных систем	ПК-26, ПК-28	З3, З4, У3, У4, Н3, Н4
Тема 2.1. Управление безопасность ОС.		
Тема 2.2. Идентифицирующие средства защиты.		
Тема 2.3. Локализующие средства защиты.		
Тема 2.4. Превентивные средства защиты.		
Тема 2.5. Восстанавливающие средства защиты.		
Зачет	ПК-24, ПК-26, ПК-28	З2-З4, У2-У4
Экзамен	ПК-24, ПК-26, ПК-28	З2-З4, У2-У4, Н2-Н4

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Организация операционных систем.								
Тема 1.1. Операционные системы.	4	2		2		2	2	
Тема 1.2. Управление задачами.	15	4		6		5	2	
Тема 1.3. Управление памятью.	19	6		6		7	2	
Тема 1.4. Управление устройствами хранения данных.	19	6		6		7	2	
Тема 1.5. Управление внешними устройствами.	15	4		6		5	2	
Тема 1.6. Управление взаимодействием	22	8		6		8	2	

Тема 1.7. Управление функциональностью.	6	2				2	2	
Раздел 2. Средства защиты операционных систем								
Тема 2.1. Управление безопасность ОС.	8	4	2			2	2	
Тема 2.2. Идентифицирующие средства защиты.	22	10	10			2	4	
Тема 2.3. Локализующие средства защиты.	20	8	10			2	2	
Тема 2.4. Превентивные средства защиты.	14	6	6			2	2	
Тема 2.5. Восстанавливающие средства защиты.	10	4	4			2	2	
Зачет	6				2	4		
Экзамен	36							36
Итого	**216 6 з.е.**	**64**	**32**	**32**	**2**	**50**	**26**	**36**

5. Содержание разделов дисциплины

5.1. Лекции

Раздел 1. Организация операционных систем

Тема 1.1. Операционные системы.

Лекция 1. Операционная система.

1. Эволюция ОС.
2. Основные функции ОС.
3. Структура и характеристики ОС.

Практическое занятие 1. Симуляторы случайных процессов.

Тема 1.2. Управление задачами

Лекция 2. Процессы.

1. Понятие процесса выполнения.
2. Состояния процесса.
3. Потоки выполнения. Принципы работы и реализации потоков.

Лекция 3. Планировщик задач.

1. Структура и принцип работы планировщика.
2. Алгоритмы планирования процессов.

Практическое занятие 2. Симулятор многозадачной системы.

Тема 1.3. Управление памятью

Лекция 4. Системная память.

1. Принципы работы буфера, кеша, свопа.
2. Диспетчер памяти: структура и принцип работы.

Лекция 5. Схемы управления памятью.

1. Способы управления памятью.
2. Алгоритмы управления страницами.

Практическое занятие 3. Симулятор виртуальной памяти.

Лекция 6. Оптимизация работы диспетчера памяти.

1. Производительность памяти, проблемы эффективности.
2. Способы оптимизации работы диспетчера памяти.

Тема 1.4. Управление устройствами хранения данных.

Лекция 7. Долговременное хранилище.

1. Файлы, каталоги, ссылки
2. Журналы и атрибуты.
3. Разбиение устройства хранения на разделы.

Лекция 8. Файловая система.

1. Назначение и структура файловой системы.
2. Виды и принципы работы файловой системы.

Практическое занятие 4. Симулятор файловой системы.

Лекция 9. Оптимизация файловой системы.
1. Виртуальная файловая система.
2. Способы оптимизации и обслуживания.

Тема 1.5. Управление внешними устройствами

Лекция 10. Периферия.
1. Архитектура подсистемы ввода вывода компьютера.
2. Абстракции ввода-вывода.
Практическое занятие 5. Симулятор периферии.
Лекция 11. Оптимизация энергопотребления.
1. Режимы и профили энергопотребления.
2. Способы снижения энергопотребления.

Тема 1.6. Управление взаимодействием

Лекция 12. Межпроцессное взаимодействие.
1. Механизмы обмена данными между процессами.
2. Проблемы и способы синхронизации процессов.
Лекция 13. Взаимоблокировки процессов.
1. Условия возникновения взаимоблокировок.
2. Способы предотвращения взаимоблокировок.
Лекция 14. Взаимодействие с пользователем
1. Интерфейс пользователя
2. Автоматизация и контроль действий
Лекция 15. Сетевая подсистема ОС.
1. Функции и структура сетевой ОС.
2. Подходы к реализации сетевого стека.
Практическое занятие 6. Симулятор сетевой системы.

Тема 1.7. Управление функциональностью.

Лекция 16. Расширения ядра ОС.
1. Модули и драйверы ОС.
2. Системные вызовы.

Раздел 2. Средства защиты операционных систем

Тема 2.1. Управление безопасность ОС.

Лекция 1. Безопасность ОС.
1. Понятие защищенной операционной системы.
2. Фрагментарный и комплексный подходы к созданию защищенных ОС.
3. Основные функции подсистемы защиты ОС.
Лекция 2. Угрозы ОС.
1. Виды атак на ОС.
2. Классификация мер защиты.

Тема 2.2. Идентифицирующие средства защиты

Лекция 3. Паролирование.
1. Метрики пароля.
2. Средства хранения и управления паролями.
Лекция 4. Инфраструктура открытых ключей.
1. Цифровой сертификат.
2. Структура PKI.
Лекция 5. Сетевая аутентификация.
1. Проблемы и принципы удаленной аутентификации.
2. Протоколы аутентификации по сети.
Лекция 6. Биометрия и карты доступа.
1. Биометрические способы идентификации.
2. Токены: назначение, виды, принцип работы.
Лекция 7. Многофакторная аутентификация.

1. Стандарт X/Open Single Sign-on (XSSO).
2. Единый расширяемый механизм управления аутентификацией. (PAM)

Тема 2.3. Локализующие средства защиты.

Лекция 8. Монитор безопасности ОС.
1. Политика безопасности ОС
2. Системы принудительного контроля доступа.

Лекция 9. Системы изолирования приложений.
1. Назначение и основные возможности «песочниц».
2. Принцип работы «песочниц».

Лекция 10. Шифрование файловой системы.
1. Достоинства и недостатки шифрования файловой системы.
1. Способы шифрования файловой системы.

Лекция 11. Программно-аппаратные замки.
1. Назначение и основные возможности программно-аппаратных замков.
2. Принцип работы программно-аппаратных замков.

Тема 2.4. Превентивные средства защиты.

Лекция 12. Антивирусы.
1. Классификация зловредных программ.
2. Принципы и методы работы антивирусов.

Лекция 13. Системы обнаружения и предотвращения нежелательных действий.
1. Назначение и основные возможности системы обнаружения и предотвращения нежелательных действий.
2. Принцип работы систем обнаружения и предотвращения нежелательных действий.

Лекция 14. Система контроля целостности.
1. Назначение и основные возможности системы контроля целостности.
2. Способы контроля и восстановления целостности системных файлов.

Тема 2.5. Восстанавливающие средства защиты

Лекция 15. Резервные копии.
1. Виды резервных копий.
2. Принципы создания резервных копий.

Лекция 16. Восстановление удалённых данных.
1. Способы безвозвратного удаления данных.
2. Способы восстановления удаленных данных.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторное занятие 1. Обнаружение уязвимостей ОС.	2
Лабораторное занятие 2. Перебор паролей.	2
Лабораторное занятие 3. Цифровая подпись	4
Лабораторное занятие 4. PAM.	4
Лабораторное занятие 5. Права доступа.	2
Лабораторное занятие 6. Изолирование приложений.	4
Лабораторное занятие 7. Шифрование каталога.	4
Лабораторное занятие 8. Безопасная загрузка.	2
Лабораторное занятие 9. Антивирус.	2
Лабораторное занятие 10. Обнаружение изменений.	4
Лабораторное занятие 11. Восстановление файлов.	2

Итого	32

5.3. Вопросы для самостоятельной работы студента.

Раздел 1. Организация операционных систем.

1. Создание экзоядра ОС с модульной архитектурой.
2. Создание модуля ядра ОС, реализующего диспетчеризацию процессов.
3. Создание модуля ядра ОС, реализующего диспетчеризацию памяти.
4. Создание модуля ядра ОС, реализующего диспетчеризацию ввода-вывода.
5. Создание модуля ядра ОС, реализующего функции виртуальной файловой системы.
6. Реализация примитивов синхронизации между потоками.
7. Реализация примитивов обмена данными между процессами.
8. Реализация примитивов обмена данными между ОС по сети.

Раздел 2. Средства защиты операционных систем.

1. Создание утилиты для хранения, генерации и оценки паролей.
2. Создание инфраструктуры PKI.
3. Разработка протокола двухсторонней аутентификации.
4. Создание приложения для идентификации пользователя через веб-камеру.
5. Создание приложения для мониторинга процессов.
6. Создание утилиты для резервного копирования.
7. Создание утилиты для восстановления файлов.
8. Создание утилиты для проверки состояния средств хранения данных.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской).

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;

– практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

– лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной

дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на экзамене и зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме экзамена и зачета. Принимается экзамен и зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Что такое ОС?
2. Какая аппаратная поддержка необходима ОС?
3. Что такое микроядерная архитектура?
4. Методы измерения производительности.
5. Что такое процесс?
6. Принцип работы псевдопараллельного режима.
7. Основные состояния процесса.
8. Принцип работы многопоточного режима.
9. Основные алгоритмы планирования.
10. Особенности алгоритмов планирования СРВ.
11. Зачем нужны средства IPC?
12. Что такое состояние гонки/состязания процессов?
13. Почему не возможна абсолютная защита с помощью бита блокировки?
14. Что такое семафор?
15. Принцип работы условных переменных?
16. Что такое граф использования ресурсов.
17. Условия ресурсной взаимоблокировки?
18. Как работает динамическое уклонение от взаимоблокировки?
19. Принцип буферизации.
20. Принцип кеширования.
21. Что такое LRU, NFU?
22. Принцип свопирования.
23. Способы описания областей в свопе?
24. Принцип работы MMU при страничном управлении памятью.
25. Что такое пробуксовка памяти?
26. Что такое TLB?
27. Для чего нужны workset-ы?
28. Что такое файл?
29. Зачем нужны жёсткие ссылки?
30. Особенности журналов.
31. Зачем нужны разделы?
32. Обобщённая структура ФС?

33. Способы размещения файлов в ФС?
34. Что такое иноды?
35. Принцип работы журнальной ФС.
36. Что такое VFS?
37. Способы оптимизации ФС?
38. Архитектура блока ввода-вывода компьютера.
39. Уровни ПО ввода-вывода.
40. Для чего нужны драйверы.
41. Для чего используется спуллинг.
42. Достоинства и недостатки потоков ввода-вывода.
43. Для чего нужны системные вызовы.
44. Факторы влияющие на управление энергопотреблением.
45. Что такое энергопрофиль системы.
46. Способы снижения энергопотребления устройств.
47. Что такое информация. Особенности информации. ИБ. КЦД.
48. Способы обеспечения ИБ. Классификация средств защиты ОС.
49. Принципы проектирования защищенных систем.
50. Понятие защищенной операционной системы.
51. Административные меры защиты. Адекватная политика безопасности.
52. Принципы паролирования.
53. Что такое PKI?
54. Принципы аутентификации с помощью биометрии и карт доступа
55. Виды сетевых протоколов аутентификации.
56. Принцип работы монитора безопасности.
57. Принцип работы "песочниц".
58. Способы шифрования файловых систем.
59. Возможности программно-аппаратных замков.
60. Методы работы антивирусов.
61. Методы работы Host-based Intrusion Prevention System(HIPS).
62. Методы работы Data Leak Prevention(DLP).
63. Правила резервного копирования.
64. Способы гарантированного уничтожения информации.

7.2. Оценивание результатов зачета

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания и лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно» (п.2.1). Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания и лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

7.3. Вопросы к экзамену

1. Операционная система: определение, функции, виды.
2. Аппаратная поддержка необходимая для ОС.
3. Принцип сквозного аргумента.
4. Виды архитектур ОС.
5. Метрики производительности ОС.

6. Методы измерения производительности.
7. Вычислительный процесс: определение, основные состояния процесса.
8. Псевдопараллельный режим: принцип работы.
9. Потоки выполнения: определение, виды, свойства.
10. Многопоточный режим: способы реализации.
11. Планировщик процессов: структура, принцип работы.
12. Алгоритмы планирования процессов.
13. Механизмы межпроцессного взаимодействия.
14. Состояние гонки/состязания процессов, условия возникновения.
15. Семафоры и мьютексы: назначение, принцип работы.
16. Принцип работы условных переменных.
17. Взаимоблокировки процессов. Условия возникновения ресурсной взаимоблокировки.
18. Способы предотвращения взаимоблокировок.
19. Принцип работы буфера, кеша, свопа.
20. Диспетчер памяти: структура, принцип работы.
21. Алгоритмы управления страницами памяти.
22. Способы оптимизации управления памятью.
23. Файл, каталог, ссылка: назначение, виды.
24. Журналы, атрибуты: назначение, виды.
25. Обобщенная структура ФС.
26. Способы размещения файлов в ФС.
27. Журнальная ФС: структура, принцип работы.
28. Способы оптимизации и обслуживания ФС.
29. Архитектура блока ввода-вывода компьютера.
30. Уровни ПО ввода-вывода.
31. Драйверы и модули: назначение, способы реализации.
32. Достоинства и недостатки потоков ввода-вывода.
33. Системные вызовы: виды, способы реализации.
34. Способы управления энергопотреблением устройств.
35. Защищенная ОС: понятие, подходы к созданию.
36. Угрозы ОС. Виды атак на ОС. Классификация мер защиты.
37. Паролирование: достоинства и недостатки, принципы работы.
38. Критерии оценки паролей. Средства управления паролями.
39. PKI: назначение, структура, принцип работы.
40. Цифровые сертификаты: структура, виды, основные операции.
41. Сетевая аутентификация: назначение, проблемы, принцип работы.
42. Аутентификация с помощью биометрии: достоинства и недостатки, принцип работы.
43. Аутентификация с помощью карт доступа: достоинства и недостатки, принцип работы.
44. Многофакторная аутентификация: определение, способы реализации в ОС.
45. Политика безопасности ОС: цели и задачи, возможности, достоинства и недостатки.
46. Принцип работы монитора безопасности. Виды правил.
47. «Песочницы»: цели и задачи, возможности, принцип работы.
48. Среда выполнения программ. Виды и способы изоляции программ.
49. Шифрование файловых систем: цели и задачи, достоинства и недостатки, способы реализации.
50. Паролирование и шифрование файлов. Правила применения шифраторов.
51. Программно-аппаратные замки: цели и задачи, возможности, принцип работы.
52. Защита процесса инициализации компьютера: этапы инициализации, уязвимости, способы устранения уязвимостей.
53. Классификация зловредных программ.

54. Методы работы антивирусов.
55. Системы обнаружения и предотвращения вторжений: цели и задачи, достоинства и недостатки.
56. Методы работы Host-based Intrusion Prevention System (HIPS).
57. Системы защиты от утечек данных: цели и задачи, достоинства и недостатки.
58. Методы работы Data Leak Prevention (DLP).
59. Резервное копирование: цели и задачи, достоинства и недостатки.
60. Виды резервных копий. Правила резервного копирования.
61. Способы гарантированного уничтожения информации.
62. Способы восстановления удаленных данных.
63. Система контроля целостности: цели и задачи, достоинства и недостатки, принцип работы.
64. Проверка целостности системных файлов. Реализация атомарности операций.

7.4. Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература.

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Таненбаум Эндрю Современные операционные системы: Питер / Таненбаум Эндрю, [пер. с англ. А. Леонтьев] - 2-е изд. - Санкт-Петербург [и др.]: Питер, 2007. - 1037с.: ил. - (Классика computer science). - ISBN 978-5-318-00299-1.
2.	Гостев, И. М. Операционные системы : учебник и практикум для академического бакалавриата / И. М. Гостев. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 164 с. Режим доступа : www.biblio-online.ru/book/A14759F4-CD1C-441C-A929-64B9D29C6010.
3.	Симаков А. Л. Защита в операционных системах: лабораторный практикум : [для 3 курса подготовки бакалавров "Информатика и вычислительная техника"] / Симаков А. Л., [отв. ред. Обломов И. А.] ; Чуваш. гос. ун-т им. И. Н. Ульянова - Чебоксары: Изд-во Чуваш. ун-та, 2013. - 35с.. - ISBN rus.

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Тони Хаулет Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям [Электронный ресурс] : учебное пособие / Хаулет Тони. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 608 c. — 978-5-4487-0065-1. — Режим доступа: http://www.iprbookshop.ru/67392.html
2.	Сафонов В.О. Основы современных операционных систем [Электронный ресурс] / В.О. Сафонов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 826 c. Режим доступа: http://www.iprbookshop.ru/62818.html
3.	UNIX . Руководство системного администратора / Эви Немет, Гарт Снайдер, Скотт Сибасс, Трент Р. Хейн. - 3-е изд. - Санкт-Петербург [и др.] : Питер, 2007. - 924с.

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Windows/ Arch linux	лицензия университета/ свободное лицензионное соглашение (https://www.archlinux.org/download/)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Виртуальная машина	лицензия университета/ свободное лицензионное соглашение (https://www.virtualbox.org/wiki/Downloads)
	свободное лицензионное соглашение	
4.	Zabbix	https://www.zabbix.com/download
5.	Clonezilla	https://clonezilla.org/downloads.php
6.	rsync	https://rsync.samba.org/

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	
3.	Журнал «Информационная безопасность»	http://www.itsec.ru/main.php
	База международных журналов **Springer Science**	
4.	International Journal of Information Security	https://link.springer.com/journal/10207
5.	Security Informatics	https://link.springer.com/journal/13388
6.	Encyclopedia of Cryptography and Security	https://link.springer.com/referencework/10.1007/978-1-4419-5906-5
7.	Advances in Information Security	https://link.springer.com/bookseries/5576

8.3.3 Нормативные методические документы в области информационной безопасности

№ п/п	Наименование
1.	Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 № 119. Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.
2.	Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. № 119.

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
3.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
4.	Xgu.ru.	http://xgu.ru/wiki/
5.	Российская Государственная Библиотека	http://www.rsl.ru
6.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
7.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
8.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
9.	Научная электронная библиотека	http://elibrary.ru
10.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
11.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.