**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"**

Институт приоритетных технологий

Кафедра информационной безопасности

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование
дисциплины (модуля): **Защита в операционных системах**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Никишова А. В., кандидат технических наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

**1. Цель и задачи изучения дисциплины**

Цель изучения дисциплины - Целью освоения дисциплины является теоретическая и практическая подготовка выпускника в области эксплуатации современных операционных систем для обеспечения их эффективного применения с учетом требований информационной безопасности

Задачи дисциплины:

- получение навыков использования методов обеспечения защиты информации в операционных системах
- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности операционных систем

**2. Место дисциплины в структуре ОПОП ВО**

Дисциплина «Защита в операционных системах» относится к обязательной части учебного плана.

Дисциплина изучается на 3 курсе.

**3. Требования к результатам освоения дисциплины**

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

**- 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**

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем

Студент должен владеть навыками:

навыками настройки политики безопасности основных операционных систем и локальных компьютерных сетей, построенных на базе основных операционных систем

**4. Объем дисциплины и виды учебной работы**

| Вид учебной работы | Всего часов | Пятый семестр |
|---|---|---|
| **Контактная работа (всего)** | **68** | **68** |
| Лабораторные | 34 | 34 |
| Лекции | 34 | 34 |

| | | |
|---|---|---|
| **Самостоятельная работа (всего)** | **40** | **40** |
| **Виды промежуточной аттестации** | **36** | **36** |
| Экзамен | 36 | 36 |
| **Общая трудоемкость часы** | **144** | **144** |
| **Общая трудоемкость зачетные единицы** | **4** | **4** |

**5. Содержание дисциплины**

**5.1. Содержание дисциплины: Лабораторные (34 ч.)**

**Пятый семестр. (34 ч.)**

Тема 1. Операционная система Windows Server 2022 (2 ч.)

Ознакомиться с основными возможностями Windows Server 2022.

Тема 2. Установка операционной системы Windows Server 2022 (2 ч.)

Получить практические навыки установки Windows Server 2022.

Тема 3. Active Directory Domain Services. Проектирование структуры (2 ч.)

Изучить и установить роли AD, Основы службы каталогов AD. Компоненты AD DS. Отношения доверия AD DS.

Тема 4. Active Directory Domain Services. Проектирование структуры (2 ч.)

Изучить и установить роли DNS и DHCP. Служба DNS. Служба DHCP.

Тема 5. Принципалы безопасности (2 ч.)

Получить навыки создания и настройки учетных записей пользователей. Создание пользователей при помощи оснастки Active Directory – пользователи и компьютеры. Настройка атрибутов учетных записей пользователей. Изменение атрибутов на вкладках свойств учетной записи пользователя. Просмотр и изменение атрибутов, не отображаемых в свойствах объектов пользователей. Создание пользователей на основании шаблонов. Создание пользователей средствами командной строки.

Тема 6. Принципалы безопасности (2 ч.)

Получить навыки создания и настройки групп. Создание групп при помощи оснастки Active Directory – пользователи и компьютеры. Создание групп средствами командной строки.

Тема 7. Присоединение ОС Windows к домену ОС Windows Server (2 ч.)

Совместная работа с Windows 10. Получить навыки присоединения клиентского компьютера, работающего под управлением Windows 10 к домену, работающему под управлением Windows Server 2022.

Тема 8. Присоединение ОС Windows к домену ОС Windows Server (2 ч.)

Совместная работа с Windows 10. Получить навыки присоединения клиентского компьютера, работающего под управлением Windows 10 к домену, работающему под управлением Windows Server 2022.

Тема 9. Организационные единицы (2 ч.)

Получить навыки делегирования административных прав. Определение и назначение организационных единиц. Создание подразделения в домене и делегирование ему полномочий на управление учетными записями. Делегирование подразделению специальные права на администрирование.

Тема 10. Управление групповыми политиками (2 ч.)

Получить навыки управления групповыми политиками. Управление групповыми политиками. Создание и редактирование объектов групповой политики. Редактирование, поиск и удаление объекта групповой политики. Включение BranchCache на клиентских компьютерах с помощью групповой .политики. Связывание объектов GPO. Принудительные связи объектов групповых политик.

Тема 11. Мониторинг событий в системе безопасности Windows (2 ч.)

Получение навыков мониторинга событий в системе безопасности Windows Server. События в

Windows. Настройка аудита. Включение аудита безопасности с помощью консоли Локальная политика безопасности. Конфигурирование аудита безопасности для доступа к файлам, принтерам и
ключам системного реестра. Определение предмета аудита.

Тема 12. Мониторинг событий в системе безопасности Windows (2 ч.)

Журналы событий в Windows. Свойства событий. Работа с журналами событий. Оснастка «Просмотр событий». Настраиваемые представления, сортировка, группировка, фильтрация, подписка на события, задачи для событий.

Тема 13. Безопасность на транспортном уровне. (2 ч.)

Механизмы защиты и шифрования информации на транспортном уровне. IPSec, инфраструктуры общедоступных ключей (PKI) и виртуальных частных сетей (VPN). Служба сертификации Active Directory (Active Directory Certificate Services — AD CS) и служба управления правами Active Directory (Active Directory Rights Management Services — AD RMS) Windows. Развертывание инфраструктуры открытых ключей с помощью Windows Server.

Тема 14. Безопасность на транспортном уровне. Службы сертификации Active Directory (2 ч.)

Установка и настройка службы сертификации AD CS. Роли центров сертификации в AD CS. Настройка автоматического развертывания.

Тема 15. Применение протокола IPSec (2 ч.)

Шифрование IPSec. Принцип работы IPSec. Основные возможности IPSec. Настройка IPSec.

Тема 16. Резервное копирование и восстановление данных (2 ч.)

Средства организации резервного копирования Windows Server. Разработать политику резервного копирования в ОС.

Тема 17. Резервное копирование и восстановление данных (2 ч.)

Настройка резервного копирования в ОС Windows Server.

**5.2. Содержание дисциплины: Лекции (34 ч.)**

**Пятый семестр. (34 ч.)**

Тема 1. Общие вопросы защиты в операционных системах (2 ч.)

Принципы проектирования защищенных систем. Понятие защищенной операционной системы. Подходы к созданию защищенных операционных систем. Административные меры защиты. Адекватная политика безопасности. Стандарты безопасности операционных систем. Политика безопасности операционных систем.

Тема 2. Модели безопасности основных операционных систем (2 ч.)

Механизмы защиты операционных систем. Анализ выполнения современными ОС формализованных требований к защите информации от НСД. Основные встроенные механизмы защиты ОС и их недостатки.

Тема 3. Угрозы безопасности операционной системы (2 ч.)

Анализ и классификация угроз безопасности ОС. Анализ существующей статистики угроз для современных универсальных ОС. Семейства ОС и общая статистика угроз.

Тема 4. Атаки на современные операционные системы (2 ч.)

Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика.

Тема 5. Анализ подсистемы безопасности в ОС семейства Windows (2 ч.)

Основные механизмы защиты в ОС семейства Windows. Принципиальные недостатки защитных механизмов ОС семейства Windows.

Тема 6. Анализ подсистемы безопасности в ОС семейства UNIX (2 ч.)

Основные механизмы защиты в ОС семейства UNIX. Особенности организации файловой системы в UNIX. Принципиальные недостатки защитных механизмов ОС семейства UNIX.

Тема 7. Идентификация, аутентификация и авторизация пользователей ОС (2 ч.)

Понятия идентификации, аутентификации и авторизации пользователей. Идентификация и аутентификация с помощью имени и пароля. Средства и методы повышения защищенности от

угрозы компрометации паролей. Идентификация и аутентификация с помощью внешних носителей ключевой информации. Идентификация и аутентификация с помощью биометрических характеристик пользователей, проблемы практической реализации данного механизма аутентификации.

Тема 8. Идентификация, аутентификация и авторизация в ОС семейства Windows (2 ч.)

Механизм идентификации пользователей. Идентификатор защиты SID пользователей. Защита объектов системы. Дескриптор безопасности SD. Атрибуты дескриптора безопасности. Парольная аутентификация в ОС семейства Windows. Механизм аутентификации. Средства управления параметрами аутентификации. Учетные записи пользователей. Локальные учетные записи пользователей. База данных SAM. Организация защиты SAM от несанкционированного доступа. Авторизация в ОС семейства Windows. Недостатки в организации разграничения доступа к файлам в ОС семейства Windows. Механизм авторизации в ОС семейства Windows. Маркеры доступа. Дескриптор безопасности. Список контроля доступа ACL. Системный (SACL) и пользовательский (DACL) списки управления доступом. Структура списков управления доступом.

Возможность управления правами доступа с помощью API. Изменение прав доступа к объекту. Смена владельца объекта. Команда cacls и ее параметры.

Тема 9. Идентификация, аутентификация и авторизация в ОС семейства UNIX (2 ч.)

Особенности подсистемы безопасности в ОС семейства UNIX. Единая модель безопасности для ОС семейства UNIX. Парольная аутентификация в UNIX. Содержимое файла /etc/passwd. Подключаемые модули аутентификации PAM. Основы PAM. Настройка PAM. Механизм идентификации пользователей. Идентификаторы пользователей UID, RUID, EUID. Учетный файл зарегистрированных групп /etc/group. Идентификаторы групп пользователей GID, RGID, EGID. Суперпользователи и привилегированные группы. Авторизация в ОС семейства UNIX. Особенности доступа к файлам в ОС семейства UNIX. Классы доступа к файлу. Список прав доступа к файлу. Изменение прав доступа к файлу утилитой chmod. Проверка прав доступа при обращении к файлам в ОС UNIX. Дополнительные права SUID, SGID, Sticky-бит. Применение дополнительных прав. Работа из-под root. Выполнение операций от имени root. Команда su и утилита sudo. Файл sudoers. Редактирование файла sudoers с помощью утилиты visudo.

Тема 10. Реализация системы безопасности сети в ОС Windows (2 ч.)

Утилиты по настройке сети. Угрозы сетевой безопасности, реализация брандмауэров. Настройка брандмауэра Windows. Защита доступа к сети.

Тема 11. Разграничение доступа к объектам ОС (2 ч.)

Требования к правилам разграничения доступа. Избирательное разграничение доступа. Изолированная программная среда. Полномочное разграничение доступа без контроля информационных потоков. Полномочное разграничение доступа с контролем информационных потоков.

Тема 12. Роли ОС Windows Server. Реализация доменных служб ActiveDirectory (2 ч.)

Развертывание на основе ролей. Развертывание серверов с конкретными ролями. Знакомство с доменными службами ActiveDirectory, реализация доменных служб AD, управление пользователями, группами, компьютерами, внедрение групповой политики. Понятие леса, домена.

Тема 13. Защита в операционной системе Windows (2 ч.)

Объекты и субъекты доступа. Субъекты доступа, которые поддерживает ОС Windows NT. Разграничение доступа в ОС Windows NT. Особенности идентификации, аутентификации и авторизации пользователей в ОС Windows NT. Аудит в ОС Windows NT. Процессы-серверы в ОС Windows NT. Особенности системы защиты Windows 2000.

Тема 14. Защита в операционной системе UNIX (2 ч.)

Защита целостности структур данных ядра в однопроцессорной системе ОС UNIX. Защита целостности структур данных ядра в многопроцессорной системе ОС UNIX. Реализации правил использования безопасных паролей в ОС UNIX. Защита файловой системы в ОС UNIX. Контроль целостности системы UNIX. Средства аудита в ОС UNIX. Особенности защиты в операционной системе Linux.

Тема 15. Аудит в ОС (2 ч.)

Необходимость аудита. Требования к подсистеме аудита. Политика аудита. Организация аудита.

Тема 16. Аудит в ОС семейства Windows (2 ч.)

Подсистема аудита в ОС семейства Windows. Категории аудита. Оснастка gpedit.msc. Настройка списка SACL. API функции для работы с SACL. Просмотр событий аудита. Утилита Event Viewer. Оснастка eventvwr.msc. Журналы аудита. Типы
регистрируемых событий в журналах аудита. Настройка журналов аудита. Типы записей в журналах событий. Определение набора подлежащих аудиту событий.

Тема 17. Аудит в ОС семейства UNIX (2 ч.)

Подсистема аудита в UNIX. Централизованная система регистрации системных сообщений Syslog. Возможности системы Syslog. Компоненты Syslog. Работа системы Syslog. Файл конфигурации Syslog syslog.conf. Селекторы Syslog. Средства и уровни Syslog. Действия с сообщениями Syslog.
Утилита newsyslog. Работа утилиты newsyslog. Файл конфигурации newsyslog.conf.

## 6. Виды самостоятельной работы студентов по дисциплине

**Пятый семестр (40 ч.)**

Вид СРС: Подготовка рефератов (20 ч.)

Тематика заданий СРС:

Тематика рефератов:

1. Механизм идентификации пользователей в ОС семейства UNIX.
2. Механизм аутентификации пользователей в ОС семейства UNIX.
3. Подключаемые модули аутентификации PAM и работе с ними в ОС семейства UNIX.
4. Механизм разграничения доступа к файлам в ОС семейства UNIX.
5. Система шифрования файлов PGP в ОС семейства UNIX.
6. Конфигурация подсистемы защиты в ОС семейства UNIX.
7. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства UNIX.
8. Bash-скрипты и работа с ними в ОС семейства UNIX.
9. Возможности усиления подсистемы безопасности в ОС семейства UNIX.
10. Ведение и анализ журналов безопасности в ОС.

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.
Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.
Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.
Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата.
1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят

данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Вид СРС: Подготовка презентации на заданную тему (20 ч.)

Тематика заданий СРС:

Тематика презентаций:
1. Механизм идентификации пользователей в ОС семейства Windows.
2. Механизм аутентификации пользователей в ОС семейства Windows.
3. Механизмы разграничения доступа к файлам в ОС семейства Windows.
4. Файловая система EFS в ОС семейства Windows.
5. Шифрования дисков BitLocker в ОС семейства Windows.
6. Служба UAC в ОС семейства Windows.
7. Шаблоны безопасности в ОС семейства Windows.
8. Подсистема защиты в ОС семейства Windows.
9. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства Windows.
10. Возможности усиления подсистемы безопасности в ОС семейства Windows.

Мультимедийная (электронная/учебная) презентация - это логически связанная последовательность слайдов, объединенных одной тематикой и общими принципами оформления. Мультимедийная презентация представляет сочетание компьютерной анимации, графики, видео, музыки и звукового ряда, которые организованы в единую среду. Чаще всего демонстрация презентации проецируется на большом экране, реже - раздается собравшимся как печатный материал.
Алгоритм самостоятельной работы по подготовке презентации на заданную тему:
1) Ознакомьтесь е предлагаемыми темами презентаций.
2) Ознакомьтесь со списком рекомендуемой литературы и источников и подготовьте их для работы.
3) Повторите лекционный материал по теме презентации (при наличии).
4) Изучите материал, касающийся темы презентации не менее чем по двум-трём рекомендованным источникам.
5) Составьте план-сценарий презентации, запишите его.
6) Проработайте найденный материал, выбирая только то, что раскрывает пункты плана презентации.
7) Составьте, наберите на компьютере и распечатайте текст своего устного выступления. При защите презентации он и будет являться сценарием презентации.
8) Продумайте дизайн презентации.
9) Подготовьте медиафрагменты (аудио-, видеоматериалы, текст и т.п.)
10) Оформите презентацию в соответствии с рекомендациями. Обязательно учтите возможные типичные ошибки и постарайтесь избежать их при создании своей презентации. Внимательно проверьте текст на отсутствие ошибок и опечаток.
11) Проверьте на работоспособность все элементы презентации.
12) Прочтите текст своего выступления медленно вслух, стараясь запомнить информацию.

13) Восстановите последовательность изложения текста сообщения, пересказав его устно.
14) Еще раз устно проговорите своё выступление в соответствии с планом, теперь уже сопровождая своё выступление демонстрацией слайдов па компьютере, делая в тексте пометки в тех местах, где нужна смена слайда.
15) Будьте готовы ответить на вопросы аудитории по теме Вашего сообщения.
К критериям оценки самостоятельной работы по подготовке презентации относятся:
Критерии оценки содержания презентации:
- соответствие материала презентации заданной теме;
- грамотное использование терминологии;
- обоснованное применение эффектов визуализации и анимации;
- общая грамотность;
- логичность изложения материала, доказательность, аргументированность.
Критерии оценки оформления презентации:
- творческий подход к оформлению презентации;
- прослеживается обоснованная последовательность слайдов и информации на слайдах;
- необходимое и достаточное количество фото- и видеоматериалов, учет особенностей восприятия графической (иллюстративной) информации, корректное сочетание фона и графики;
- дизайн презентации не противоречит ее содержанию;
- грамотное соотнесение устного выступления и компьютерного сопровождения, общее впечатление от мультимедийной презентации.

## 7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

## 8. Фонд оценочных средств. Оценочные материалы

### 8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

| Уровень сформированности компетенции | Шкала оценивания для промежуточной аттестации | Шкала оценивания по БРС |
|---|---|---|
| | Экзамен, зачет с оценкой | |
| Повышенный | 5 (отлично) | 91 и более |

| | | |
|---|---|---|
| Базовый | 4 (хорошо) | 71 – 90 |
| Пороговый | 3 (удовлетворительно) | 60 – 70 |
| Ниже порогового | 2 (неудовлетворительно) | Ниже 60 |

Критерии оценки знаний студентов по дисциплине

| Оценка | Показатели |
|---|---|
| Отлично | Обучающийся демонстрирует:<br>систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы;<br>точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы;<br>безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;<br>выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации;<br>полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине;<br>умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин;<br>творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий. |
| Хорошо | Обучающийся демонстрирует:<br>систематизированные, глубокие и полные знания по всем разделам учебной дисциплины;<br>использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;<br>владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач;<br>способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями;<br>усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине;<br>умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку;<br>активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий. |

| | |
|---|---|
| Удов-летвори-тельно | Обучающийся демонстрирует:<br>достаточные знания в объеме рабочей программы по учебной дисциплине;<br>использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок;<br>владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;<br>способность самостоятельно применять типовые решения в рамках изучаемой дисциплины;<br>усвоение основной литературы, рекомендованной рабочей программой по дисциплине;<br>умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине;<br>работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий. |
| Неудов-летвори-тельно | Обучающийся демонстрирует:<br>фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине;<br>неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок;<br>пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий. |

**8.2. Вопросы, задания текущего контроля**

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

**- 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**

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем

Вопросы, задания:

1. Механизм аутентификации пользователей в ОС семейства Windows.
2. Мониторинг и аудит событий безопасности в ОС.
3. Настройка брандмауэра ОС.

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем

Задания:

1. Настроить параметры политики безопасности в ОС.
2. Разработать политику безопасности ОС.
3. Настроить парольную политику ОС.

Студент должен владеть навыками:

навыками настройки политики безопасности основных операционных систем и локальных компьютерных сетей, построенных на базе основных операционных систем

Задания:

1. Установить и настроить операционную систему под заданные требования безопасности.
2. Настроить учетные записи ОС в соответствии с заданными требованиями безопасности.
3. Настроить разграничение доступа в соответствии с заданными требованиями безопасности.

**8.3. Вопросы промежуточной аттестации**

**Пятый семестр (Экзамен)**

1. Угрозы безопасности операционных систем.
2. Классификация угроз безопасности операционных систем.
3. Стандарты безопасности операционных систем.
4. Политики безопасности операционных систем.
5. Понятие защищенной операционной системы.
6. Административные меры защиты. Адекватная политика безопасности.
7. Механизмы защиты операционных систем.
8. Обзор и статистика методов, лежащих в основе атак на современные ОС.
9. Изолированная программная среда.
10. Избирательное разграничение доступа.
11. Субъекты, объекты и права доступа.
12. Правила разграничения доступа.
13. Идентификация, аутентификация и авторизация пользователей.

**8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Пятый семестр

1. Контрольная работа - от 0 до 35 баллов
2. Устный опрос, собеседование - от 0 до 30 баллов
3. Письменные задания или лабораторные работы - от 0 до 35 баллов
4. Экзамен - от 0 до 40 баллов

## 9. Перечень основной и дополнительной учебной литературы

### 9.1 Основная литература

1. Астахова Ирина Федоровна Компьютерные науки. Деревья, операционные системы, сети [Электронный ресурс]: учебное - ФИЗМАТЛИТ, 2013. - 88 с. - Режим доступа: http://znanium.com/go.php?id=428176

2. Назаров С.В., Гудыно Л.П., Кириченко А.А. Операционные системы [Электронный ресурс]: учебное - КноРус, 2016. - 372 с. - Режим доступа: https://www.book.ru/book/920515

### 9.2 Дополнительная литература

1. Партыка Татьяна Леонидовна Операционные системы, среды и оболочки [Электронный ресурс]: учебное - Издание перераб. и доп. - ФОРУМ, 2017. - 560 с. - Режим доступа: http://new.znanium.com/go.php?id=552493

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

### 9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.edu.ru. - Федеральный портал «Российское образование»

2. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю

**10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов**

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:

- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

**11. Перечень информационных технологий**

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

**11.1 Перечень программного обеспечения**
**(обновление производится по мере появления новых версий программы)**

Перечень лицензионного и свободно распространяемого
программного обеспечения*:
Microsoft Windows 10 PRO. Номер лицензии: 65946188
Microsoft Office профессиональный 2016. Номер лицензии:
нет. Номер договора 31604241628.2016 от 21.11.2016 г.
Kaspersky Endpoint Security. Номер лицензии:
280E-201102-083042-350-950
7-zip-открытая лицензия
Adope Acrobat Reader – открытая лицензия

Программное обеспечение:
1. Microsoft Windows 7 Professional, 11 лицензий, номер
60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия,
OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
5. LibreOffice 12 лицензий (свободно-распространяемое
программное обеспечение)
6. FreeBSD, 1 лицензия FreeBSD license свободное программное
обеспечение
7. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное
программное обеспечение
8. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL)
свободное программное обеспечение
9. Visual Studio Community 2017, 13 лицензий, учебное

программное обеспечение
10. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)

**11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы (обновление выполняется еженедельно)**

| Название | Краткое описание | URL-ссылка |
|---|---|---|
| Научная электронная библиотека | Крупнейший российский информационный портал в области науки, технологии, медицины и образования. | http://elibrary.ru/ |
| ЭБС "Лань" | Электронно-библиотечная система | https://e.lanbook.com/ |
| ЭБС Znanium.com | Электронно-библиотечная система | https://znanium.com/ |
| ЭБС BOOK.ru | Электронно-библиотечная система | https://www.book.ru/ |
| ЭБС Юрайт | Электронно-библиотечная система | https://www.biblio-online.ru/ |
| Scopus | Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства. | http://www.scopus.com/ |
| Web of Science | Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок. | https://apps.webofknowledge.com/ |
| КонсультантПлюс | Информационно-справочная система | http://www.consultant.ru/ |
| Гарант | Информационно-справочная система по законодательству Российской Федерации | http://www.garant.ru/ |
| Научная библиотека ВолГУ им О.В. Иншакова | | http://library.volsu.ru/ |

**12. Материально-техническое обеспечение дисциплины**

Специализированная мебель:
Парта со скамьей- 106 шт.
Учебные места - 260 шт.
Рабочее место преподавателя (стол и стул) – 3 шт.
Доска аудиторная-1 шт.
Технические средства обучения:
Компьютерный комплекс кафедры мультимедийной -1 шт.
Мультимедийная кафедра -1 шт.
Мультимедийный проектор (EIKI EK DLP Projector EK-625U) -1 шт.

Интерактивная доска-1 шт.

Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.