**УТВЕРЖДЕНО**
решением Ученого совета ФМИАТ
от «21» 06 2019 г., протокол № 5/19
Председатель _____ Волков М.А.
*(подпись, расшифровка подписи)*
«21» 06 2019 г.

# РАБОЧАЯ ПРОГРАММА

| | |
|---|---|
| Дисциплина | Защита в операционных системах |
| Факультет | Математики, информационных и авиационных технологий |
| Кафедра | Информационной безопасности и теории управления |
| Курс | 4 |

Специальность: 10.05.01 «Компьютерная безопасность»
*код направления (специальности), полное наименование*

Специализация: «Математические методы защиты информации»
*полное наименование*

Форма обучения: очная
*очная, заочная, очно-заочная (указать только те, которые реализуются)*

Дата введения в учебный процесс УлГУ: «01» сентября 2018 г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.

Сведения о разработчиках:

| ФИО | Кафедра | Должность, ученая степень, звание |
|---|---|---|
| Клочков Андрей Евгеньевич | ИБиТУ | Старший преподаватель |
| | | |

| СОГЛАСОВАНО | СОГЛАСОВАНО |
|---|---|
| Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину | Заведующий выпускающей кафедрой «Информационная безопасность и теория управления» |
| / _____ / Андреев А.С. /<br>*(подпись)* *(Ф.И.О.)*<br>«19» 06 2019г. | / _____ / Андреев А.С. /<br>*(подпись)* *(Ф.И.О.)*<br>«19» 06 2019г. |

## 1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

**Цели освоения дисциплины:**

- приобретение общих представлений о реализации механизмов защиты информации в современных операционных системах;
- знакомство с основными концепциями организации безопасности на уровне операционных систем.

**Задачи освоения дисциплины:**

- изучение различных подходов реализации безопасности на уровне файловых систем и систем хранения данных;
- дать основы системного подхода к организации аутентификации и авторизации пользователей;
- дать основы системам проведения аудитов безопасности операционных систем.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита в операционных системах» относится к обязательной части Блока 1 «Дисциплины (модули)» Основной Профессиональной Образовательной Программы специалитета по специальности 10.05.01 – «Компьютерная безопасность», специализация «Математические методы защиты информации» (Б1.О.1.1.37).

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов информатики, основ информационной безопасности, аппаратных средства вычислительной техники, операционных систем, сетей и систем передачи данных.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как «Защита программ и данных», «Основы построения защищенных компьютерных сетей», «Основы построения защищенных баз данных», «Модели безопасности компьютерных систем».

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Защита в операционных системах» направлен на формирование следующих компетенций.

| Код и наименование реализуемой компетенции | Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций |
|---|---|
| ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. | Знать:<br>Основные виды угроз информационной безопасности операционной системы.<br>Основные системы защиты информации в операционных системах. Существующие средства защиты информации.<br>Владеть:<br>Терминологией по защите информации. |
| ОПК-12 – Способен администрировать операционные системы и выполнять работы по восстановлению | Знать:<br>Руководящие документы по описанию системы защиты объекта информатизации. |

| | |
|---|---|
| работоспособности прикладного и системного программного обеспечения. | Механизмы проведения аудита информационной безопасности. Методы сбора журналов событий.<br>Руководящие документы по организации защиты операционных систем от НСД и НДВ.<br>Особенности современных программно-аппаратных комплексов защиты информации.<br>Методы реализации функций обеспечения целостности данных в современных операционных системах.<br>Уметь:<br>Формировать техническую документацию на защиту операционной системы.<br>Настраивать и анализировать журналы информационной безопасности.<br>Настраивать работу операционной системы с применением средств защиты информации.<br>Восстанавливать целостность данных на основе современных программно-аппаратных комплексов. |
| ОПК-13 – Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности. | Знать:<br>Механизмы практической реализации защиты информации.<br>Различные подходы к решению задач по защите операционных систем.<br>Методы анализа уязвимостей современных операционных система.<br>Уметь:<br>Правильно настраивать системы защиты информации для операционных систем.<br>Выявлять и ранжировать угрозы информационной безопасности.<br>Комплексно применять механизмы защиты информации для операционной системы.<br>Владеть:<br>Навыками работы с современными реализациями механизмов защиты информации.<br>Возможностями современного прикладного программного обеспечения для защиты ОС. |

## 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

**4.1. Объем дисциплины в зачетных единицах (всего) 4.**

**4.2. Объем дисциплины по видам учебной работы (в часах):**

| **Вид учебной работы** | Количество часов (форма обучения: *очная*) | |
|---|---|---|
| | **Всего по плану** | **В т.ч. по семестрам** |
| | | **7** |
| 1 | 2 | 3 |
| Контактная работа обучающихся с преподавателем в соответствии с УП | **72/72*** | **72/72*** |
| Аудиторные занятия | **72/72*** | **72/72*** |
| Лекции | **36/36*** | **36/36*** |
| Практические и семинарские занятия | | |

| | | |
|---|---|---|
| Лабораторные работы (лабораторный практикум) | **36/36*** | **36/36*** |
| Самостоятельная Работа | **36** | **36** |
| Форма текущего контроля знаний и контроля самостоятельной работы. | Лабораторные работы | Лабораторные работы |
| Курсовая работа | **0** | **0** |
| Контроль | **36** | **36** |
| Виды промежуточной аттестации | – | экзамен |
| Всего часов по дисциплине | **144** | **144** |

**В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.*

**4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:**

Форма обучения _____очная_____

| **Название разделов и тем** | **Всего** | **Виды учебных занятий** | | | | | **Форма текущего контроля знаний** |
|---|---|---|---|---|---|---|---|
| | | **Аудиторные занятия** | | | **Занятия в интерактивной форме** | **Самостоятельная работа** | |
| | | **Лекции** | **Практические занятия, семинары** | **Лабораторные работы, практикумы** | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | |
| **Раздел 1. Защита информации в современных информационных системах** | | | | | | | |
| 1. Основные понятия и положения защиты информации в информационно-вычислительных системах | 8 | 6 | | 0 | 0 | 2 | Защита лабораторной работы |
| 2. Угрозы безопасности информации в информационновычислительных системах. | 12 | 8 | | 0 | 0 | 4 | Защита лабораторной работы |
| 3. Программнотехнический уровень обеспечения информационной безопасности и его организация. | 14 | 8 | | 0 | 0 | 6 | Защита лабораторной работы |
| **Раздел 2. Подсистема безопасности в ОС семейства Windows** | | | | | | | |
| 4. Анализ подсистемы безопасности в ОС семейства Windows | 7 | 2 | | 2 | 1 | 2 | Защита лабораторной работы |

| | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Идентификация, аутентификация и авторизация в ОС семейства Windows | 17 | 1 | | 8 | 6 | 2 | Защита лабораторной работы |
| 6. Аудит в ОС семейства Windows. | 6 | 1 | | 2 | 1 | 2 | Защита лабораторной работы |
| 7. Возможности шифрования файлов в ОС семейства Windows | 10 | 2 | | 4 | 2 | 2 | Защита лабораторной работы |
| 8. Прочие возможности подсистемы безопасности в ОС семейства Windows | 6 | 1 | | 2 | 1 | 2 | Защита лабораторной работы |
| 9. Усиление подсистемы безопасности в ОС семейства Windows | 6 | 1 | | 2 | 1 | 2 | Защита лабораторной работы |
| **Раздел 3. Подсистема безопасности в ОС семейства UNIX** | | | | | | | |
| 10. Анализ подсистемы безопасности в ОС семейства UNIX. | 9 | 3 | | 2 | 2 | 2 | Защита лабораторной работы |
| 11. Идентификация, аутентификация и авторизация в ОС семейства Windows. | 17 | 1 | | 8 | 6 | 2 | Защита лабораторной работы |
| 12. Аудит в ОС семейства UNIX | 7 | 1 | | 2 | 2 | 2 | Защита лабораторной работы |
| 13. Возможности шифрования файлов в ОС семейства UNIX с использованием PGP. | 13 | 1 | | 4 | 2 | 6 | Защита лабораторной работы |
| Итого | 108 | 36 | | 36 | 24 | 36 | |
| Контроль | 36 | | | | | 36 | Экзамен |
| **Всего** | **144** | | | | | | |

## 5. СОДЕРЖАНИЕ КУРСА

**Раздел 1. Защита информации в современных информационных системах.**

**Тема 1. Основные понятия и положения защиты информации в информационно вычислительных системах.** Предмет защиты информации. Понятия информации и информационных ресурсов. Достоверность, ценность и своевременность информации. Предмет защиты информации. Объект защиты информации. Понятия информационной системы. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности информационных систем. Трехэтапная разработка мер по обеспечению безопасности информационных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные

принципы обеспечения информационной безопасности в автоматизированной системе (АС). Положения по защите АС. Принципы, позволяющие реализовать положения по защите АС. Принцип системности. Принцип комплексности. Принцип непрерывной защиты. Разумная достаточность. Гибкость системы защиты. Открытость алгоритмов и механизмов защиты. Принцип простоты применения средств зашиты.

**Тема 2. Угрозы безопасности информации в информационно-вычислительных системах.** Понятие угрозы. Понятие атаки. Понятие злоумышленника. Источники угроз. Окно опасности. Критерии классификации угроз. Базовые признаки угроз информационной безопасности. Классификация угроз по природе возникновения. Классификация угроз по степени преднамеренности проявления. Классификация угроз по непосредственному источнику угроз. Классификация угроз по положению источника угроз. Классификация угроз по степени зависимости от активности АС. Классификация угроз по степени воздействия на АС. Классификация угроз по этапам доступа пользователей или программ к ресурсам АС. Классификация угроз по способу доступа к ресурсам АС. Классификация угроз по текущему месту расположения информации, хранимой и обрабатываемой в АС. Доступность информации. Угроза доступности. Целостность информации. Угроза нарушения целостности. Конфиденциальность информации. Угроза нарушения конфиденциальности. Угроза раскрытия параметров АС. Методы обеспечения информационной безопасности. Структуризация методов обеспечения информационной безопасности. Уровни доступа к защищаемой информации. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников.

**Тема 3. Программно-технический уровень обеспечения информационной безопасности и его организация**. Подходы к обеспечению компьютерной безопасности. Сервис безопасности. Основные и вспомогательные сервисы безопасности. Понятие полного набора. Виды сервисов безопасности. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации. Проблема надежной аутентификации и пути ее решения. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Парольная аутентификация. Виды парольной аутентификации. Преимущества и недостатки парольной аутентификации. Повышение надежности парольной аутентификации. Средства и методы защиты от компрометации и подбора паролей. Биометрическая аутентификация. Общая схема биометрической аутентификации. Преимущества и недостатки биометрической аутентификации. Достоинства и недостатки различных схем биометрической аутентификации. Требования к защите компьютерной информации. Общие положения. Характеристики подходов к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к набору и параметрам механизмов защиты. Необходимые требования. Дополнительные требования. Формализованные требования к защите информации от несанкционированного доступа. Общие подходы к построению систем защиты компьютерной информации. Нормативные документы Гостехкомиссии РФ, регламентирующие защиту информации от несанкционированного доступа. Формализованные требования к защите компьютерной информации АС. Основные подсистемы и группы механизмов защиты АС. Требования к защите конфиденциальной информации. Требования к защите секретной информации. Различия требований и основополагающих механизмов защиты от несанкционированного доступа.

## Раздел 2. Подсистема безопасности в ОС семейства Windows.

**Тема 4. Анализ подсистемы безопасности в ОС семейства Windows.**

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

**Тема 5. Идентификация, аутентификация и авторизация в ОС семейства Windows.** Возможности подсистемы безопасности в ОС семейства Windows. Модель безопасности для подсистемы безопасности в ОС семейства Windows. Механизм идентификации пользователей. Идентификатор защиты SID пользователей. Идентификаторы полномочий. Возможные значения идентификатора полномочий. Относительный идентификатор. Маркер доступа и привилегии пользователя. Просмотр привилегий пользователя. Команда whoami и ее параметры.

Ограничивающие маркеры доступа. Команда runas и ее параметры. API функции для создания маркеров доступа. 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. Возможности получения доступа к 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. Формат дескрипторов безопасности. Список контроля доступа ACL. Системный (SACL) и пользовательский (DACL) списки управления доступом. Структура списков управления доступом. Возможность управления правами доступа с помощью API. Пример проверки прав доступа пользователя к объекту. Изменение прав доступа к объекту. Смена владельца объекта. Команда cacls и ее параметры.

**Тема 6. Аудит в ОС семейства Windows.** 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 7. Возможности шифрования файлов в ОС семейства Windows.** Шифрующая файловая система EFS. Возможности шифрующей файловой системы EFS. Принципы работы EFS. Используемые в EFS алгоритмы шифрования. Случайный ключ для шифрования файла FEK. Шифрование ключа FEK. Команда cipher и ее параметры. Понятие агента восстановления. Добавление агентов восстановления. Сертификаты агентов восстановления. Поле восстановления данных DRF. API функции для работы с EFS. Система шифрования дисков BitLocker. Основные возможности BitLocker. Поддерживаемые алгоритмы шифрования. Принцип работы. Механизмы проверки подлинности и расшифровки. Уязвимости BitLocker. Настройка BitLocker. Шифрование и дешифрование дисков при помощи BitLocker.

**Тема 8. Прочие возможности подсистемы безопасности в ОС семейства Windows.**

Интерфейс CryptoAPI. Возможности CryptoAPI. Работа с поставщиками службы шифрования CSP. Типы CSP в ОС семейства Windows. Контроль учетных записей пользователей UAC. Предпосылки к появлению UAC. Принцип работы UAC. События, приводящие к срабатыванию UAC. Настройка UAC. Недостатки UAC. Шаблоны безопасности в ОС семейства Windows. Возможности шаблонов безопасности. Настройки шаблонов безопасности.

**Тема 9. Усиление подсистемы безопасности в ОС семейства Windows.**

Использование систем криптографической защиты информации. Наиболее известные системы криптографической защиты информации и особенности их работы. Противодействие вирусным атакам в системе. Выбор антивируса. Организация антивирусной защиты.

**Раздел 3. Подсистема безопасности в ОС семейства UNIX**

**Тема 10. Анализ подсистемы безопасности в ОС семейства UNIX.**

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

**Тема 11. Идентификация, аутентификация и авторизация в ОС семейства UNIX.**

Особенности подсистемы безопасности в ОС семейства UNIX. Единая модель безопасности для ОС семейства UNIX. Парольная аутентификация в UNIX. Зарегистрированные пользователи системы. Учетный файл зарегистрированных пользователей /etc/passwd. 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. Возможности суперпользователей и привилегированных групп. Хранение паролей в других файлах в ОС семейства UNIX. Командные интерпретаторы в ОС семейства UNIX. Авторизация в ОС семейства UNIX. Особенности доступа к файлам в ОС семейства UNIX. Классы доступа к файлу. Список прав доступа к файлу. Различие возможных значений прав доступа для разных типов файлов. Изменение прав доступа к файлу утилитой chmod. Формат команд для утилиты chmod. Проверка прав доступа при обращении к

файлам в ОС UNIX. Дополнительные права SUID, SGID, Sticky-бит. Применение дополнительных прав. Работа из-под root. Особенности работы из-под root. Выполнение операций от имени root. Команда su и утилита sudo. Файл sudoers. Редактирование файла sudoers с помощью утилиты visudo.

**Тема 12. Аудит в ОС семейства UNIX.**

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. Тема 13. Возможности шифрования файлов в ОС семейства UNIX с использованием PGP. Шифование файлов при помощи PGP. Особенности PGP. Защищенность PGP. Ключи, генерируемые PGP и их типы. Поддержка PGP возможности цифровой подписи и сжатия данных. Установка и настройка PGP.

**Тема 13. Возможности шифрования файлов в ОС семейства UNIX с использованием PGP.**

## 6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Не предусмотрены учебным планом дисциплины.

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторная работа №1. Пользователи и группы.

Цель. Изучение системы администрирования пользователей и групп в операционных системах. Изучение системы защиты информации файловых систем NTFS (MS Windows) и ext4fs (BaseAlt (Альт Рабочая станция, Альт сервер)). Реализация системы разграничение прав доступа к каталогам файловой системы и файлам. Разграничение прав доступа к файловой системе по сети.

Лабораторная работа №2. Массовая регистрация пользователей.

Цель. Изучение системы администрирования пользователей при помощи стандартного API операционной системы. Изучение методов назначения прав доступа к объектам файловой системы из скриптовых языков.

Лабораторная работа №3. Политика безопасности.

Цель. Изучение возможности управления групповой политики операционных систем семейства Microsoft Windows.

Лабораторная работа №4. Ограниченное использование программ.

Цель. Изучение возможности изменения уровней безопасности операционной системы путем блокирования определённых приложений.

Лабораторная работа №5. Взлом паролей пользователей.

Взлом паролей Microsoft Windows 10.

Лабораторная работа №6. Прозрачное шифрование файловой системы.

Цель. Изучение возможностей применения «прозрачного» шифрования данных в файловых системах.

Лабораторная работа №7. Шифрование и хеширование.

Цель. Изучение методов контроля целостности и шифрования данных.

Лабораторная работа №8. Отказоустойчивость. RAID массивы.

Цель. Изучение возможностей программный средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации.

Лабораторная работа №9. Домены.

Цель. Изучение возможностей создания контура безопасности предприятия на основе доменной

структуры. Применение групповых политик безопасности к пользователям и компьютерам предприятия.

Лабораторная работа №10. Аудит событий.

Цель. Изучение механизмов регистрации различных событий в ОС. Ознакомление с методами анализа событий по различным критериям.

## 8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Не предусмотрены учебным планом дисциплины.

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Основные понятия и положения защиты информации в информационно вычислительных системах.
2. Угрозы безопасности информации в информационно-вычислительных системах и их классификацию.
3. Основные понятия программно-технического уровня обеспечения информационной безопасности.
4. Основные сервисы безопасности и их особенности.
5. Требования к защите компьютерной информации с учетом различных нормативных документов.
6. Принципиальные недостатки защитных механизмов ОС семейства Windows.
7. Механизм идентификации пользователей в ОС семейства Windows.
8. Механизм аутентификации пользователей в ОС семейства Windows.
9. Механизмы разграничения доступа к файлам в ОС семейства Windows.
10. Файловая система EFS в ОС семейства Windows.
11. Шифрования дисков BitLocker в ОС семейства Windows.
12. Возможности CryptoAPI в ОС семейства Windows.
13. Служба UAC в ОС семейства Windows.
14. Шаблоны безопасности в ОС семейства Windows.
15. Подсистема защиты в ОС семейства Windows.
16. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства Windows.
17. Возможности усиления подсистемы безопасности в ОС семейства Windows.
18. Принципиальные недостатки защитных механизмов ОС семейства UNIX.
19. Механизм идентификации пользователей в ОС семейства UNIX.
20. Механизм аутентификации пользователей в ОС семейства UNIX.
21. Подключаемые модули аутентификации PAM и работе с ними в ОС семейства UNIX.
22. Механизм разграничения доступа к файлам в ОС семейства UNIX.
23. Система шифрования файлов PGP в ОС семейства UNIX.
24. Конфигурация подсистемы защиты в ОС семейства UNIX.
25. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства UNIX.
26. Bash-скрипты и работа с ними в ОС семейства UNIX.
27. Возможности усиления подсистемы безопасности в ОС семейства UNIX.
28. Ведение и анализ журналов безопасности в ОС.

## 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

| Название разделов и тем | Вид самостоятельной работы | Объем в часах | Форма контроля |
|---|---|---|---|
| Защита информации в современных информационных системах | Проработка учебного материала, выполнение лабораторных работ | 12 | Защита лабораторных работ |

| | | | |
|---|---|---|---|
| Подсистема безопасности в ОС семейства Windows | Проработка учебного материала, выполнение лабораторных работ | 12 | Защита лабораторных работ |
| Подсистема безопасности в ОС семейства UNIX | Проработка учебного материала, выполнение лабораторных работ | 12 | Защита лабораторных работ |
| | *подготовка к сдаче экзамена* | 36 | Экзамен |

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**а) Список рекомендуемой литературы**

**основная**

1. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470010.
2. Руссинович М. Соломон Д. Ионеску А. Внутреннее устройство Windows. Седьмое издание. – Санкт-Петербург, Издательство Питер 2019г. – 944 с. – ISBN 978-5-4461-0663-9.

**дополнительная**

1. Таненбаум Э. Бос. Х. Современные операционные системы. Санкт-Петербург, Издательство ПИТЕР, 2019 г. – 1120с ISBN: 978-5-4461-1155-8.
2. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / Щеглов А.Ю., Щеглов К.А.. — Санкт-Петербург : Университет ИТМО, 2015. — 93 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/67260.html — Режим доступа: для авторизир. пользователей
3. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов [и др.].. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 193 с. — ISBN 978-5-8265-1737-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/85968.html — Режим доступа: для авторизир. пользователей
4. Пушкарев В.П. Защита информационных процессов в компьютерных системах : учебное пособие / Пушкарев В.П., Пушкарев В.В.. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 131 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/13929.html — Режим доступа: для авторизир. пользователей.

**учебно-методическая**

1. Кулябов Д.С. Основы администрирования операционных систем: лабораторные работы: учебное пособие / Кулябов Д.С., Королькова А.В. — Москва: Российский университет дружбы народов, 2018. — 123 с. — ISBN 978-5-209-09058-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/104234.html — Режим доступа: для авторизир. пользователей
2. Филиппов М.В. Операционные системы : учебно-методическое пособие / Филиппов М.В., Завьялов Д.В.. — Волгоград : Волгоградский институт бизнеса, 2014. — 163 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/56020.html — Режим доступа: для авторизир. пользователей
3. Глотина И.М. Средства безопасности операционной системы Windows Server 2008 : учебно-методическое пособие / Глотина И.М.. — Саратов : Вузовское образование, 2018. — 141 с. — ISBN 978-5-4487-0136-8. — Текст : электронный // Электронно-

библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/72538.html — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/72538

Согласовано:

Гл. библ-рь ИБ УлГУ | Полина Ю.Ю | 21.06.2019

должность сотрудника научной библиотеки | ФИО | подпись | дата

**б) Программное обеспечение**

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows 10, Microsoft Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер), Kali.

**в) Профессиональные базы данных, информационно-справочные системы**

**1. Электронно-библиотечные системы:**

1.1. IPRbooks: электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2019]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст: электронный.

1.2. ЮРАЙТ: электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2019]. - URL: https://urait.ru/. – Режим доступа: для зарегистрир. пользователей. - Текст электронный.

1.3. Консультант студента: электронно-библиотечная система: сайт / ООО Политехресурс. – Москва, [2019]. – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань: электронно-библиотечная система: сайт / ООО ЭБС Лань. – Санкт-Петербург, [2019. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

1.5. Znanium.com**:** электронно-библиотечная система: сайт / ООО Знаниум. - Москва, [2019]. - URL: http://znanium.com. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

**2. Национальная электронная библиотека**: электронная библиотека : федеральная государственная информационная система: сайт / Министерство культуры РФ ; РГБ. – Москва, [2019]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

**3. SMART Imagebase** // EBSCOhost: [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа: для авториз. пользователей. – Изображение: электронные.

**4. Федеральные информационно-образовательные порталы:**

4.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/. – Текст : электронный.

4.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

**5. Образовательные ресурсы УлГУ:**

5.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5.2. Образовательный портал УлГУ. – URL: http://edu.ulsu.ru. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

зам. нач УИТ | Клочкова ВВ | | 21.06.2019

должность сотрудника УИТиТ | ФИО | подпись | дата

Помещение 2/24б. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 12). Экран настенный, мультимедийный проектор. Информационные

плакаты. Компьютер, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106 (3 корпус).

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- операционная среда ОС Windows 10, Microsoft Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер), Kali.

## 13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться некоторые из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– 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.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ ст. преподаватель кафедры Клочков Андрей Евгеньевич
подпись должность ФИО