Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1156866	Безопасность операционных систем

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Информационная безопасность телекоммуникационных систем 2. Информационно-аналитические системы безопасности	**Код ОП** 1. 10.05.02/22.01 2. 10.05.04/22.01
Направление подготовки 1. Информационная безопасность телекоммуникационных систем; 2. Информационно-аналитические системы безопасности	**Код направления и уровня подготовки** 1. 10.05.02; 2. 10.05.04

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Зубков Евгений Валерьевич	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Безопасность операционных систем

1.1. Аннотация содержания модуля

Модуль «Безопасность операционных систем» содержит в себе дисциплины операционные системы и обеспечение безопасности операционных систем, в которых излагается устройство и особенности эксплуатации операционных систем со всеми штатными элементами и службами безопасности. Изучаются основные файловые системы, способы безопасного хранения системных программ и данных, модули аутентификации пользователей, сетевые службы и защищенные технологические режимы. Завершается модуль дисциплиной, излагающей принципы проектирования отечественной ОС Astra Linux.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Операционные системы	3
2	Обеспечение безопасности операционных систем	4
	ИТОГО по модулю:	7

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Информатика
Постреквизиты и кореквизиты модуля	1. Безопасность баз данных 2. Защита информации

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Обеспечение безопасности операционных систем	ПК-1 - Способен решать типовые задачи анализа информации в ИАС государственных органов,	З-1 - Излагать методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования

	обеспечивающих национальную безопасность **(Информационная безопасность телекоммуникационных систем)**	З-2 - Определять способы измерения свойств объектов предметной области З-3 - Описывать методы теории вероятностей, теории случайных процессов и математической статистики З-4 - Применять математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС З-5 - Описывать программное обеспечение процесса решения задач анализа информации в ИАС З-6 - Объяснять организационные меры по защите информации У-1 - Проверять гипотезы и границы их применения в задачах анализа информации в ИАС У-2 - Представлять результаты решения аналитических задач в стандартном виде У-3 - Применять математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС У-4 - Применять методические подходы к интерпретации профессионального смысла получаемых результатов анализа информации в ИАС П-1 - Разрабатывать математические модели и методы решения задач анализа информации в ИАС, создавая соответствующее программное и математическое обеспечение П-2 - Иметь практический опыт определения границ их применения и подтверждения или опровержения их на практике П-3 - Иметь практический опыт решения типовых задач анализа информации в ИАС П-4 - Иметь практический опыт интерпретации профессионального смысла получаемых формальных результатов
	ПК-1 - Способен разрабатывать методики	З-1 - Описывать методики выполнения аналитических работ

	выполнения аналитических работ **(Информационно-аналитические системы безопасности)**	У-1 - Проводить апробацию методик на выбранных проектах и их доработках У-2 - Разрабатывать рекомендации по изменению аналитических систем П-1 - Иметь опыт выявления проблем и сложностей в существующих аналитических работах организации
Операционные системы	ПК-1 - Способен решать типовые задачи анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность **(Информационная безопасность телекоммуникационных систем)**	З-1 - Излагать методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования З-2 - Определять способы измерения свойств объектов предметной области З-3 - Описывать методы теории вероятностей, теории случайных процессов и математической статистики З-4 - Применять математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС З-5 - Описывать программное обеспечение процесса решения задач анализа информации в ИАС З-6 - Объяснять организационные меры по защите информации У-1 - Проверять гипотезы и границы их применения в задачах анализа информации в ИАС У-2 - Представлять результаты решения аналитических задач в стандартном виде У-3 - Применять математические модели, методы и алгоритмы решения типовых задач анализа информации в ИАС У-4 - Применять методические подходы к интерпретации профессионального смысла получаемых результатов анализа информации в ИАС П-1 - Разрабатывать математические модели и методы решения задач анализа информации в ИАС, создавая соответствующее программное и математическое обеспечение

		П-2 - Иметь практический опыт определения границ их применения и подтверждения или опровержения их на практике П-3 - Иметь практический опыт решения типовых задач анализа информации в ИАС П-4 - Иметь практический опыт интерпретации профессионального смысла получаемых формальных результатов
	ПК-1 - Способен разрабатывать методики выполнения аналитических работ **(Информационно-аналитические системы безопасности)**	З-1 - Описывать методики выполнения аналитических работ У-1 - Проводить апробацию методик на выбранных проектах и их доработках У-2 - Разрабатывать рекомендации по изменению аналитических систем П-1 - Иметь опыт выявления проблем и сложностей в существующих аналитических работах организации

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Операционные системы

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Зубков Евгений Валерьевич	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Зубков Евгений Валерьевич, Доцент,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Общие принципы безопасности операционных систем	Ключевые элементы программной архитектуры операционных систем. Защищенные файловые системы. Модель безопасности и ее архитектура. Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС. Безопасность системных данных. Способы защиты системных файлов от незаконной модификации. Управление памятью. Механизмы виртуальной памяти. Создание и уничтожение процессов. Аудит событий безопасности
2	Защита компьютерной информации в операционных системах Linux	Файл как универсальный объект ОС. Загрузчики операционных систем. Архитектура файловых систем. Атрибуты процесса. Использование возможностей командных оболочек при решении штатных задач администрирования. Пользователи и их виды.

		Копирование и запись данных. Архивация и резервирование. Сетевые возможности операционных систем. Наблюдение и аудит в ОС Linux. Основные ошибки и просчеты в администрировании компьютерных сетей под управлением операционных систем Linux. Анализ настроек безопасности UNIXсистем.
3	Защита компьютерной информации в операционных системах семейства Windows	ОС Windows. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows. Разграничение доступа в ОС Windows. Структура системного реестра ОС Windows. Редактирование реестра. Анализ и настройка политики безопасности. Аудит событий безопасности. Анализ сетевых служб Windows. Использование инструментальных средств аудита безопасности компьютерных систем.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-1 - Способен решать типовые задачи анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность	З-5 - Описывать программное обеспечение процесса решения задач анализа информации в ИАС

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Операционные системы

Электронные ресурсы (издания)

1. Синадский, Н. И., Бакланов, В. В.; Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие.; [ГОУ ВПО УГТУ-УПИ], Екатеринбург; 2007 (70 экз.)

Печатные издания

1. Синицын, С. В., Батаев, А. В., Налютин, Н. Ю.; Операционные системы : учеб. для студентов вузов, обучающихся по специальности "Прикладная информатика (по областям)" и др. экон. специальностям.; Академия, Москва; 2010 (6 экз.)

2. Синицын, С. В., Михайлов, А. С., Хлытчиев, О. И.; Программирование на языке высокого уровня : учеб. для студентов вузов, обучающихся по специальности "Прикладная информатика (по обл.)" и др. экон. специальностям.; Академия, Москва; 2010 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

1. Министерство образования науки Российской Федерации (http:_минобрнауки.рф_)

2. Федеральный портал_ Российское образование_(http:_ www.edu.ru_)

3. ООО Научная электронная библиотека (http:_elibrary.ru_defaultx.asp)

4. Зональная научная библиотека УрФУ (http:_lib.urfu.ru)

5. Электронный научный архив УрФУ (http:_elar.urfu.ru_)

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Операционные системы

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
2	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	**Не требуется**
3	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
5	Самостоятельная работа студентов	Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Обеспечение безопасности операционных систем

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Зубков Евгений Валерьевич	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Зубков Евгений Валерьевич, Доцент,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Общие принципы безопасности операционных систем	Ключевые элементы программной архитектуры операционных систем (ОС), определяющие защиту компьютерной информации и безопасность ЭВМ. Архитектура многозадачной сетевой операционной системы. Уровень ядра и уровень приложений. Объекты ядра. Аппаратно–зависимый программный слой. Защищенные файловые системы. Владение файловыми объектами и права доступа к ним. Изменение разрешений на доступ к файлам. Размещение элементов файловой системы на дисковом пространстве. Типовые файловые системы. Структура и назначение метаданных файлов. Понятие политики разграничения доступа в компьютерных системах. Одноуровневая и многоуровневая модели разграничения доступа, их достоинства и недостатки. Реализация технологии разграничения доступа в операционных системах. Модель безопасности и ее архитектура. Администрирование учетных записей пользователей. Группы пользователей. Права и привилегии пользователей и групп.

		Управление системной политикой безопасности. Стратегия предоставления прав на доступ к ресурсам. Хранение парольной информации. Алгоритм сетевой аутентификации. Обеспечение безопасности при удаленном доступе. Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС. Безопасность системных данных. Способы защиты системных файлов от незаконной модификации. Управление памятью. Механизмы виртуальной памяти. Создание и уничтожение процессов. Управление процессами и контроль над ними. Реализация многозадачного и многопоточного режимов. Механизмы системных вызовов. Защита на уровне межпроцессного взаимодействия. Сокрытие процессов. Реализация защитных требований на уровне командной оболочки. Защита программного обеспечения от незаконной модификации. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора
2	Защита компьютерной информации в операционных системах Linux и FreeBSD	Ключевые элементы программной архитектуры ОС, влияющие на защиту информации. Базовые понятия. Основные отличия операционных систем Linux и FreeBSD. Файл как универсальный объект ОС. Виды файлов. Права доступа к файлам. Основные команды, позволяющие работать с файлами. Действия над обычными файлами: создание, копирование, перемещение, удаление. Работа с каталогами. Создание и изменение разрешений на доступ к файлам. Использование «жестких» и символических ссылок. Дополнительные атрибуты файлов, поддерживаемые в ОС Linux. Работа со специальными файлами устройств. Загрузчики операционных систем LILO, GRUB. Обеспечение защиты от НСД при загрузке ОС. Вход в систему в однопользовательском режиме. Загрузка ПК с LiveCD с целью устранения неполадок. Архитектура файловых систем ext*fs и ufs*. Размещение элементов файловой системы на дисковом пространстве. Назначение и структура суперблока, описателей групп блоков, карт битовых полей, индексных дескрипторов, журнала транзакций. Структура индексного

		дескриптора регулярного файла, каталога, символической ссылки. Работа с устройствами дисковой и полупроводниковой памяти. Создание, изменение и удаление дисковых разделов. Отображение информации о дисковых разделах и файловых системах. Форматирование разделов и создание файловых систем. Конфигурационный файл /etc/fstab. Монтирование устройств и дисковых разделов с различными файловыми системами. Размещение файловых систем на дисковом пространстве. Монтирование разделов памяти с различными файловыми системами. Установление дисковых квот. Восстановление логически удаленных или поврежденных файлов. Последовательность логического удаления файлов в файловых системах ext*fs и ufs*. Виды повреждений файловой системы. Утилиты для работы с поврежденными файловыми системами. Возможности дисковых редакторов типа Linux Disk Editor и отладчиков файловых систем для восстановления утерянной компьютерной информации. Особенности восстановления файлов в различных файловых системах. Использование записей из журнальных файлов. Блочное копирование информации с поврежденных машинных носителей с помощью утилиты dd. Ключевые аргументы командной строки. Сетевое копирование с использованием утилиты netcat. Атрибуты процесса. Файловая система /proc как «зеркало» процессов. Переменные окружения. Создание и уничтожение процессов, изменение их приоритетов. Способы автоматического запуска и остановки программ. Периодически запускаемые процессы. Запуск и остановка программ в интерактивном и фоновом режимах. Средства взаимодействия между процессами. Перенаправление ввода/вывода. Терминальный режим и консольные

		атаки. Вывод информации о процессах. Наблюдение за процессами и контроль производительности системы. Признаки камуфляжа несанкционированно выполняемых процессов. Программные возможности сокрытия процессов. Использование возможностей командных оболочек 7 при решении штатных задач администрирования. Типовой синтаксис команд. Запуск программ в фоновом режиме. Запуск нескольких команд, в т.ч. по условию. Командные файлы. Перенаправление ввода и вывода. Конвейеры. Управление операционной системой в многотерминальном режиме. Работа с файловым менеджером Midnight Commander. Пользователи и их виды. Группы пользователей. Учетные записи пользователей и работа с ними. Изменение, редактирование, удаление и временное блокирование учетных записей. Конфигурационные файлы group, passwd, master.passwd, shadow, login.defs. Временные отметки и признаки паролей. Смена паролей. Процедура регистрации и ее безопасность. Смена пользователей. Предоставление эффективных прав доступа. Использование механизма SUDO. Практические задачи на разграничение доступа и их решения. Предоставление пользователям временных прав суперпользователя. Распространенные атаки на права администратора системы. Исследование учетных записей пользователей. Обнаружение неавторизованных учетных записей пользователей и групп. Копирование и запись данных. Архивация и резервирование. Сетевые возможности операционных систем. Контроль и настройка сетевых интерфейсов. Разведка узлов компьютерной сети и сетевых служб. Методы сканирования узлов ЛВС. Возможности утилиты nmap. Режимы открытого и скрытного сканирования. Перехват и анализ сетевого трафика с

		помощью утилиты tcpdump. Задание условий фильтрации трафика. Особенности настройки и проверки работоспособности узлов беспроводных сетей. Уязвимости алгоритмов криптографической защиты. Наблюдение и аудит в ОС Linux и FreeBSD. Сбор информации об опасных файловых объектах. Поиск необычных и скрытых файлов и каталогов. Наблюдение за процессами и пользователями. Отслеживание взаимосвязей между субъектами, процессами и объектами. Аудит событий и его безопасность. Системные протоколы, их расположение и заполнение. Источники, потребители и уровни значимости сообщений. Защита системы протоколирования событий. Основные ошибки и просчеты в администрировании компьютерных сетей под управлением операционных систем Linux и FreeBSD. Анализ настроек безопасности UNIX-систем
3	Защита компьютерной информации в операционных системах семейства Windows	Реализация технологии разграничения доступа в ОС Windows *. Объекты и субъекты доступа. Права и методы доступа. Дескриптор защиты. Дискреционный список контроля доступа. Системный список контроля доступа. Структура маркера доступа. Процесс проверки подлинности при входе в систему. Стратегия предоставления прав на доступ к ресурсам. Защита данных средствами разрешений файловой системы NTFS. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows*. Методы идентификации и аутентификации пользователей, применяемые в ОС Windows*. Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS. Структура зашифрованного файла. Создание ключа и сертификата агента восстановления. Хранение парольной информации. Анализ уязвимости паролей пользователей.

		Алгоритмы локальной и сетевой аутентификации. Механизмы криптографической защиты данных на логических разделах и съемных носителях информации, реализованные в ОС Windows 7. Технология BitLocker. Создание замкнутой программной среды с помощью функции AppLocker. Организация файловой системы NTFS. Основные свойства файловой системы NTFS. Структура MFT. Стандартные атрибуты файлов и каталогов в NTFS. Основные операции над объектами файловой системы. Резидентные и нерезидентные атрибуты. Потоки. Структура каталогов. Размещение файловой системы на дисковом пространстве. Разграничение доступа в ОС Windows*. Планирование и создание учетных записей пользователей и рабочих групп. Разграничение доступа к ресурсам. Разрешения доступа к общим папкам. Получение доступа к пользовательским данным с правами администратора. Структура системного реестра ОС Windows*. Редактирование реестра. Разделы и настройки системного реестра, определяющие политику безопасности. Использование реестра для настройки параметров ОС. Утилиты администрирования реестра с интерфейсом командной строки. Анализ и настройка политики безопасности. Анализ параметров безопасности. Рекомендуемые права пользователей. Управление системной политикой безопасности. Политика учетных записей. Разработка шаблона политики безопасности. Анализ и настройка политики безопасности с применением шаблонов. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора. Настройки журнала аудита. Анализ и

		восстановление данных на логических разделах NTFS. Подключение машинных носителей с NTFS-разделами. Восстановление главной загрузочной записи. Восстановление таблицы разделов и загрузочного сектора. Приемы и программное обеспечение для «ручного» восстановления удаленных файлов на NTFS разделах. Возможности автоматизированного восстановления удаленных файлов. Анализ сетевых служб Windows*. Анализ сетевых компьютеров с использованием стандартных сетевых команд. Анализ сетевых узлов с использованием программ-сканеров портов. Анализ возможности сетевого подключения к файловым ресурсам Windows*. Использование инструментальных средств аудита безопасности компьютерных систем.
4	Особенности защиты компьютерной информации в операционной системе Mac OS X	Создание, изменение и удаление учетных записей пользователей. Регистрация в системе и выход из нее. Включение и использование учетной записи суперпользователя root. Виды паролей: пароль учетной записи, пароль администратора, мастер-пароль, пароль суперпользователя. Выбор паролей с помощью Password Assistant. Пароли в виде «связки ключей». Сброс и обновление паролей. Аппаратный пароль Firmware Password. Работа с файлами. Надежное удаление файлов. Права доступа к файлам. Запрет изменений файлов. Особенности файловой системы hfsplus. Структура файлов. Восстановление поврежденных файлов. Использование механизма SUDO для предоставления пользователям дополнительных прав. Системные настройки безопасности. Шифрование пользовательских данных с помощью

		FileVault. Включение и выключение механизма шифрования. Недостатки режима шифрования. Контроль за режимом изоляции программной среды. Системная защита от вредоносных программ и сетевых атак. Загрузка операционной системы в однопользовательском режиме. Защита компьютеров Apple от непосредственного доступа. Экранная заставка. Контроль рабочего места с помощью видеорегистрации. Настройка средств сетевой защиты Mac OS X 10.6. Особенности регистрации системных событий. Расположение и безопасность журналов аудита

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-1 - Способен решать типовые задачи анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность	З-6 - Объяснять организационные меры по защите информации

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Обеспечение безопасности операционных систем

Электронные ресурсы (издания)

1. Олифер, В. Г.; Основы сетей передачи данных: вводный курс : учебное пособие.; Интернет-Университет Информационных Технологий (ИНТУИТ), Москва; 2003; https://biblioclub.ru/index.php?page=book&id=234533 (Электронное издание)

Печатные издания

1. , Андрончик, А. Н., Богданов, В. В., Домуховский, Н. А., Коллеров, А. С., Синадский, Н. И., Хорьков, Д. А., Щербаков, М. Ю.; Защита информации в компьютерных сетях. Практический курс : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем".; УГТУ-УПИ, Екатеринбург; 2008 (1 экз.)

2. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

3. Хорев, П. Б.; Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника".; Academia, Москва; 2005 (29 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Обеспечение безопасности операционных систем

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	
2	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	**Не требуется**
3	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Консультации	Мебель аудиторная с количеством рабочих мест в	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
5	Самостоятельная работа студентов	Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES