

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

*Мещеряков*  
С.Т. Князев  
27 апреля 2021 г.



## РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля  
1156866

Модуль  
Безопасность операционных систем

Екатеринбург, 2021

<b>Перечень сведений о рабочей программе модуля</b>	<b>Учетные данные</b>
<b>Образовательная программа</b> <i>Информационно-аналитические системы безопасности</i>	<b>Код ОП 10.05.04/22.01</b>
<b>Направление подготовки</b> Информационно-аналитические системы безопасности	<b>Код направления и уровня подготовки</b> <i>10.05.04</i>

Область образования, в рамках которых реализуется модуль образовательной программы по ФГОС ВО 3++, уровень *специалитет*:

<b>№ п/п</b>	<b>Перечень областей образования, для которых разработан ФГОС ВО 3++</b>	<b>Уровень подготовки</b>
1.	Инженерное дело, технологии и технические науки	<i>специалитет</i>

Программа модуля составлена авторами:

<b>№ п/п</b>	<b>Фамилия Имя Отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	<i>Учебно-научный центр «Информационная безопасность»</i>
2	Пономарева Ольга Алексеевна		Старший преподаватель	<i>Учебно-научный центр «Информационная безопасность»</i>

**Руководитель модуля - С.В. Поршнев**

**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 и часах
1.	Обеспечение безопасности операционных систем	4/144
2.	Операционные системы	3/108
ИТОГО по модулю:		7/252

### 1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Информатика
Постреквизиты и корреквизиты модуля	Защита информации в информационно-управляющих системах

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

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям. Результаты обучения формулируются глаголами в активной форме или отглагольным существительным, должны содержать индикатор/измеряемый критерий (например, самостоятельно формулировать предложения...; понимать/понимание; рассчитывать необходимое количество материалов.../ расчет необходимого количества материалов... и т.д.). При выборе глаголов полезно опираться на таксономию Блума.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 2

Код и наименование компетенции	Планируемые результаты обучения (индикаторы) [указываются в соответствии с содержанием трудовых функций из профессиональных стандартов (трудовыми действиями, необходимыми знаниями и умениями), соотносящимися с компетенцией]			
	Знания:	Умения:	Практический опыт, владение	Другие результаты (указываются при необходимости, к примеру, личностные качества)
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	<p>РО1-З ОПК1 Знает сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства "РО2-3 ОПК1 Знает психологические аспекты информационной безопасности в современном обществе"</p> <p>"РО3-3 ОПК1 Знает угрозы и источники угроз информационной безопасности современного</p>	<p>РО1-У ОПК1 Умеет применять основные методы обеспечения информационной безопасности</p>	<p>РО1-В ОПК 1 Владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества и государства</p>	

	общества" " РО4-3 ОПК1 Знает основные методы обеспечения информационной безопасности"			
--	---	--	--	--

### **1.5. Форма обучения**

Обучение по дисциплинам модуля может осуществляться в очной форме

**ПРОГРАММА МОДУЛЯ**  
*Безопасность операционных систем*

**СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1**

*Обеспечение безопасности операционных систем*

Рабочая программа дисциплины составлена авторами:

<b>№ п/п</b>	<b>Фамилия Имя Отчество</b>	<b>Ученая степень, ученое звание</b>	<b>Должность</b>	<b>Подразделение</b>
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	<i>Учебно-научный центр «Информационна я безопасность»</i>

**Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ**

## 2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

### Обеспечение безопасности операционных систем

#### 2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология (ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне);

#### 2.2.1. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Общие принципы безопасности операционных систем	<p>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.</p> <p>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.</p> <p>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.</p> <p>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. Соккрытие процессов. Реализация защитных требований на уровне командной оболочки. Защита программного обеспечения от незаконной модификации.</p>

		<p>Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора.</p>
2	<p>Защита компьютерной информации в операционных системах Linux и FreeBSD</p>	<p>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</p>



		<p>взаимодействия между процессами. Перенаправление ввода/вывода. Терминальный режим и консольные атаки. Вывод информации о процессах. Наблюдение за процессами и контроль производительности системы.</p> <p>Признаки камуфляжа несанкционированно выполняемых процессов. Программные возможности сокрытия процессов. Использование возможностей командных оболочек <code>7</code> при решении штатных задач администрирования. Типовой синтаксис команд.</p> <p>Запуск программ в фоновом режиме. Запуск нескольких команд, в т.ч. по условию. Командные файлы. Перенаправление ввода и вывода. Конвейеры.</p> <p>Управление операционной системой в многотерминальном режиме. Работа с файловым менеджером <code>Midnight Commander</code>. Пользователи и их виды. Группы пользователей. Учетные записи пользователей и работа с ними. Изменение, редактирование, удаление и временное блокирование учетных записей. Конфигурационные файлы <code>group</code>, <code>passwd</code>, <code>master.passwd</code>, <code>shadow</code>, <code>login.defs</code>. Временные отметки и признаки паролей. Смена паролей.</p> <p>Процедура регистрации и ее безопасность. Смена пользователей. Предоставление эффективных прав доступа. Использование механизма <code>SUDO</code>.</p> <p>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.</p> <p>Методы сканирования узлов ЛВС. Возможности утилиты <code>ntar</code>. Режимы открытого и скрытого сканирования. Перехват и анализ сетевого трафика с помощью утилиты <code>tcpdump</code>. Задание условий фильтрации трафика. Особенности настройки и проверки работоспособности узлов беспроводных сетей. Уязвимости алгоритмов криптографической защиты. Наблюдение и аудит в ОС <code>Linux</code> и <code>FreeBSD</code>. Сбор информации об опасных файловых объектах. Поиск необычных и скрытых файлов и каталогов.</p> <p>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 <code>Linux</code> и <code>FreeBSD</code>. Анализ настроек безопасности UNIX-систем</p>
3	Защита компьютерной информации в операционных системах	Реализация технологии разграничения доступа в ОС <code>Windows *</code> . Объекты и субъекты доступа. Права и методы доступа. Дескриптор защиты. Дискреционный

	<p>семейства Windows</p>	<p>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*.</p> <p>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.</p> <p>Алгоритмы локальной и сетевой аутентификации. Механизмы криптографической защиты данных на логических разделах и съемных носителях информации, реализованные в ОС Windows 7. Технология BitLocker.</p> <p>Создание замкнутой программной среды с помощью функции AppLocker.</p> <p>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. Поток. Структура каталогов. Размещение файловой системы на дисковом пространстве.</p> <p>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.</p> <p>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</p>
--	--------------------------	--

		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	<p>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.</p> <p>Работа с файлами. Надежное удаление файлов. Права доступа к файлам. Запрет изменений файлов. Особенности файловой системы hfsplus. Структура файлов. Восстановление поврежденных файлов.</p> <p>Использование механизма SUDO для предоставления пользователям дополнительных прав.</p> <p>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.</p> <p>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</p>

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

## 2.4.1 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 1

*Обеспечение безопасности операционных систем*

### **Электронные ресурсы (издания)**

1. Портал информационно-образовательных ресурсов УрФУ <http://study.ustu.ru/info/default.aspx>
2. Официальный сайт ИРИТ-РмФ <http://rtf.ustu.ru>
3. Официальный сайт кафедры ТОР УрФУ <http://tor.rtf.ustu.ru>

### **Печатные издания**

1. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007 .— 136 с. 90 экз.

2. 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" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.

Дополнительная литература:

3. Олифер В. Г. Сетевые операционные системы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер .— 2-е изд. — Москва [и др.] : Питер, 2008 .— 669 с. 10 экз.

4. Уайт К. Основы обслуживания Mac OS X. Руководство по обслуживанию и разрешению проблем Mac OS X 10.5 / Кевин М. Уайт ; [пер. с англ. О. Труфанова] .— Москва : ЭКОМ, 2009 .— 592 с. 1 экз

5. Пог.Д. Mac OS X Leopard. Основное руководство / Дэвид Пог ; [пер. с англ. С. Маккавеева] .— Санкт-Петербург ; Москва : Символ-Плюс, 2008 .— 880 с. 1 экз.

6. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с. 10 экз.

7. Ивановский С. Операционная система Linux: Сборник часто задаваемых вопросов и ответов на них / С. Ивановский .— М. : Познавательная книга плюс, 2001 .— 224 с. 1 экз.

8. Робачевский А.М. Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский .— Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002 .— 514 с. 9. 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. <http://www.intuit.ru/> - Национальный открытый университет «ИНТУИТ»
2. <http://www.edu.ru/> - Федеральный портал. Российское образование.
3. <http://study.ustu.ru> –портал информационно-образовательных ресурсов УрФУ
4. <http://rtf.ustu.ru> - официальный сайт ИРИТ-РтФ

## 2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Безопасность операционных систем

### Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащённость специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	<i>Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном.</i>	OS Linux, Windows, Mac OS X

		<p><i>Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet</i></p> <p><i>P-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.</i></p> <p><i>P-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.</i></p>	
--	--	--	--

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

*Операционные системы*

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	<i>Учебно-научный центр «Информационна я безопасность»</i>

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

### 3. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

#### *Операционные системы*

#### 3.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология (*ориентирована на передачу знаний и умений, обеспечивающая усвоение обучающимися содержания обучения, проверку и оценку его качества на репродуктивном уровне*);

#### 3.2. Содержание дисциплины 2

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 UNIX-систем.
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.

3.3. Программа дисциплины реализуется на государственном языке Российской Федерации

#### 3.4 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 1

##### *Операционные системы*

##### Электронные ресурсы (издания)

1. Портал информационно-образовательных ресурсов УрФУ  
<http://study.ustu.ru/info/default.aspx>
2. Официальный сайт ИРИТ-РтФ <http://rtf.ustu.ru>
3. Официальный сайт кафедры ТОР УрФУ <http://tor.rtf.ustu.ru>

#### Печатные издания

1. Сеницын С. В. *Операционные системы : учебник для вузов / С. В. Сеницын, А. В. Батаев, Н. Ю. Налютин .— 3-е изд., стер. — Москва : Издательский центр "Академия", 2013 .— 296 с.*
2. Робачевский А.М. *Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский .— Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002 .— 514 с. 12 экз.*

#### Дополнительная литература:

1. Синадский Н.И. *Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007 .— 136 с. 90 экз.*
2. 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" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.*
3. Платонов В.В. *Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с. 10 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. <http://www.intuit.ru/> - Национальный открытый университет «ИНТУИТ»
2. <http://www.edu.ru/> - Федеральный портал. Российское образование.
3. <http://study.ustu.ru> –портал информационно-образовательных ресурсов УрФУ
4. <http://rtf.ustu.ru> - официальный сайт ИРИТ-РтФ

### 3.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

#### Операционные системы

#### Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащённость специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	<i>Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование.</i>	ОС Linux, Windows,



		<p><i>Локальная сеть с выходом в глобальную сеть Internet</i> <i>P-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.</i></p> <p><i>P-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.</i></p>	
--	--	---	--