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
«29» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156874

Модуль
Защита информации

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП 10.05.02/22.01**
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** *10.05.02*

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

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

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	д.т.н., профессор	Директор УНЦ ИБ	*Учебно-научный центр «Информационная безопасность»*
2	Пономарева Ольга Алексеевна		Старший преподаватель	*Учебно-научный центр «Информационная безопасность»*

Руководитель модуля - *С.В. Поршнев*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1.

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защита информации

1.1. Аннотация содержания модуля

Модуль «Защита информации» посвящен изучению существующих программно-аппаратных средств защиты компьютерной информации и автоматизированных систем в защищенном исполнении. Изучаются основные направления защиты информации, защиты информации, обрабатываемой в распространенных клиентских приложениях, защита компьютерной информации от вредоносных программ, защита информации, хранимой на машинных носителях и специализированные программно-аппаратные средства защиты..

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.	Защита информации в компьютерных сетях	*6/216*
2	Защита информации в системах беспроводной связи	*4/144*
3	Комплексное обеспечение защиты информации в объектах информатизации	*4/144*
4	Методы резервирования и восстановления информации	*3/108*
5	Программно-аппаратные средства защиты информации	*5/180*
	ИТОГО по модулю:	*22/792*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Компьютерное моделирование
Постреквизиты и кореквизиты модуля	Государственная итоговая аттестация

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)			
	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	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-З ОПК1 Знает психологические аспекты информационной безопасности в современном обществе" "РО3-З ОПК1 Знает угрозы и источники угроз	РО1-У ОПК1 Умеет применять основные методы обеспечения информационной безопасности	РО1-В ОПК 1 Владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества и государства "РО2-В ОПК 1 Владеет базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информционной безопасности"	

	информационной безопасности современного общества" "РО4-З ОПК1 Знает основные методы обеспечения информационной безопасности"			

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
Защита информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1
Защита информации в компьютерных сетях

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	Учебно-научный центр «Информационная безопасность»

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1

Защита информации в компьютерных сетях

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. Содержание дисциплины 1

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.
2	Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows 2000-XP. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого
3	Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP.

		Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
4	Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory
5	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности.

		Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в компьютерных сетях

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

1. Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие / Н. И. Синадский. – Екатеринбург: УрГУ, 2008. – 225 с.

2. Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.

3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru
http://lib.urfu.ru/mod/data/view.php?id=1379]

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

[*список с указанием наименования баз данных, информационно-справочных и поисковых систем*]

www.consultant.ru. - www.garant.ru. - Электронно- библиотечная **система** ZNANIUM.COM – режим доступа www.znanium.com.

- Научная электронная библиотека eLIBRARY.RU – режим доступа http://elibrary.ru.
- Электронная библиотека Grebennikon – режим доступа http://grebennikon.ru/.
- Универсальная справочно-информационная полнотекстовая **база данных** периодических изданий EastViewhttp://ebiblioteka.ru/.

2.4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 1

Защита информации в компьютерных сетях

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. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном — 1 комплект;* *3. Персональные ЭВМ, объединенные в локальную вычислительную сеть Ethernet. Минимальные требования к персональным компьютерам: платформа IA-32, тактовая частота центрального процессора не ниже 2 ГГц, оперативная память объемом не менее 512 Мбайт, жесткие магнитные диски с интерфейсом Serial ATA и емкостью не менее 300 Мбайт;.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации*	1. операционные системы семейства MS Windows NT 5.0 (лицензии по числу рабочих мест); 2. программное обеспечение организации виртуальных сетей VMware Workstation (лицензии по числу рабочих мест); 3. СЗИ VPN «VipNET» 4. СЗИ VPN «StrongNET» 5. СКЗИ КриптоПро CSP

ПРОГРАММА МОДУЛЯ
Защита информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2

Защита информации в системах беспроводной связи

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	д.т.н., профессор	Директор УНЦ ИБ, профессор	Учебно-научный центр «Информационная безопасность»
	Пономарева О.А.		Ст. препод.	Департамент Информационных технологий и автоматики

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

Защита информации в системах беспроводной связи

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. Содержание дисциплины 2

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Основы построения беспроводных сетей	Беспроводные сети передачи информации. История и основные понятия. Краткий экскурс в историю беспроводной связи. Основные термины и понятия. Стандарт IEEE 802.11.Сетевая архитектура. Постановка задачи распределенной обработки данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. Основы организации и функционирования сетей. Основные сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиентсервер, одноранговые сети, локальные и глобальные сети. Неоднородные вычислительные сети.
2	Технологии обеспечения безопасности в беспроводных сетях	Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты. Влияние человеческого фактора на сетевую безопасность. Защита топологии сети. Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование. Виртуальные частные сети. Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами. Средства повышения надежности функционирования Сетей. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.
3	Проектирование защищенных	Политика безопасности Понятие политики безопасности. Типовые элементы политики

	беспроводных сетей	безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности. Критерии оценки безопасности сетевых ОС Основные критерии анализа сетевой безопасности. Общая процедура анализа. Методика подготовки экспертного заключения. Анализ угроз, уязвимостей и атак. 6 Классификация беспроводных систем, анализ состава и архи- тектурных особенностей построения БС, изучение функциональных особенностей современных стандартов БС, проектирование системы информационной безопасности БС на основе моделирования ключе- вых процессов при помощи аппарата анализа рисков.
4	Методы и алгоритмы прогнозирования эффективности защиты БС	Анализ угроз, уязвимостей и атак. Классификация беспроводных систем, анализ состава и архитектурных особенностей построения БС, изучение функциональных особенностей современных стандартов БС, проектирование системы информационной безопасности БС на основе моделирования ключевых процессов при помощи аппарата анализа рисков. Анализ возможных сценариев атак. Постановка задачи оценки эффективности наборов средств защиты беспроводных сетей. Риск-анализ беспроводных сетей Разработка рискшанс модели компонентов беспроводных сетей группы стандартов IEEE 802.11.Анализ эффективности. Оценка эффективности системы обеспечения безопасности беспроводных сетей группы стандартов IEEE 802.11.Механизмы управления Организация и управление экспертной системой для оценки основных показателей защищенности беспроводной сети Оптимизация выбора мер и средств защиты Методический подход к оптимизации выбора мер и средств защиты беспроводных сетей группы стандартов IEEE 802.11

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

Электронные ресурсы (издания)

- *ЭБС, на которые есть подписка,*
- *elar.urfu.ru,*
- *study.urfu.ru,*
- *иные сайты в домене urfu.ru.*

Сведения берутся из электронного каталога библиотеки http://lib.urfu.ru/course/view.php?id=76 и включаются в рабочую программу после проверки их доступности (должен открываться полный текст, а не ознакомительный фрагмент).]

Печатные издания

1. Проскурин, В.Г.. Защита программ и данных : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 090900 "Информ. безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информ. Безопасность автоматизир. систем" / В. Г. Проскурин .— Москва : Академия, 2011 .— 208 с. (25 экз.)

2. Ермаков, Д.Г. Применение антивирусных программ для обеспечения информационной безопасности : учебное пособие для студентов, обучающихся по программе бакалавриата по направлениям подготовки 080500 "Бизнес-информатика", 230700 "Прикладная информатика", 080100 "Экономика" / Д. Г. Ермаков, А. В. Присяжный ; Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина .— Екатеринбург : Издательство Уральского университета, 2013 .— 64 с (5 экз.)

3. Платонов, Владимир Владимирович. Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / В. В. Платонов .— Москва : Академия, 2013— 336 с. (5 экз.)

Дополнительная литература:

1. Е.А. Степанов Информационная безопасность и защита информации : Учеб. для студентов вузов / Е. А. Степанов, И. К. Корнеев .— Москва : ИНФРА-М, 2001 .— 304 с. (25 экз.)

2. В. А. Копылов. Информационное право : Учебник / В. А. Копылов ; Моск. гос. юрид. акад. — 2-е изд., перераб. и доп. — Москва : Юристъ, 2002 .— 512 с. ; 22 см .— (institutiones) .— Библиогр. в примеч, библиогр.: с. 506-510 (5 экз)

3. Теоретические основы компьютерной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем", "Информ. безопасность телеком. систем" / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков .— М. : Радио и связь, 2000 (4 экз.)

4. Баранова, Е.К.. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш .— Москва : КНОРУС, 2015

Методические разработки

1. Гуляев, В.П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации : учебно-методический комплект для студентов, обучающихся по направлению 090106.65-Информационная безопасность телекоммуникационных систем / В. П. Гуляев ; Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина .— Екатеринбург : Издательство Уральского университета, 2014 .— 164 с. (5 экз.)

Программное обеспечение

Microsoft Word

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.urfu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.urfu.ru - официальный сайт ИРИТ-РтФ

Электронные образовательные ресурсы

Не предусмотрено

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.

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 2

Защита информации в системах беспроводной связи **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. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet* *4. Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.

ПРОГРАММА МОДУЛЯ
Защита информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 3
Комплексное обеспечение защиты информации в объектах информатизации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Виноградова Нина Сергеевна	-	Ст. преп.	Радиоэлектроники и связи

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 3

Комплексное обеспечение защиты информации в объектах информатизации

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. Содержание дисциплины 3

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Теоретические основы компьютерной безопасности	Основные понятие и предметная область информационной безопасности (ИБ), ее место в системе национальной безопасности Российской Федерации. Особенности информации как объекта защиты. Основные свойства и виды защищаемой информации. Источники и носители защищаемой информации. Роль человеческого фактора в информационной системе Классификация категорий пользователей и других лиц по их влиянию на безопасность компьютерной информации. Социально психологический портрет хакера. Анализ и классификация угроз ИБ, виды ущерба от реализовавшихся угроз и его последствия. Основные направления информационной защиты. Силы, средства и методы и обеспечения информационной безопасности объектов. Политика информационной безопасности. Системы ограничения и разграничения доступа к защищаемым данным. Основные модели разграничения доступа. Политика разграничения доступа.
2	Криптографические методы защиты информации	Основные понятия криптографии: алгоритмы и ключи шифрования; простейшие шифры и их свойства: шифры простой замены, перестановки, гаммирования; теорема Шеннона; блоковые и потоковые шифры; современные стандарты шифрования; атаки на криптосистему; теоретическая и практическая криптостойкость шифров; имитостойкость и помехоустойчивость шифров. Принципы построения криптографических алгоритмов с открытыми ключами. Сравнительная характеристика систем симметричного и несимметричного шифрования.

		Алгоритмы DES и ГОСТ 28147-89; асимметричные криптосистемы с открытыми ключами; понятие необратимых и односторонних функций; схема открытого распределения ключей Диффи-Хеллмана; стандарты функций хэширования России и США. Электронная подпись (ЭП); способы организации ЭП; аутентификация сообщений и пользователей в современных системах информационных технологий на базе ЭП; применение хэш-функций в схемах ЭП. Стандарты ЭП России и США. Особенности аппаратной и программной реализации современных криптосистем. Средства шифрования, предоставляемые прикладными программами офисного пакета.
3	Программно-аппаратные средства обеспечения информационной безопасности	Методы и средства ограничения доступа к компонентам ЭВМ и входа в систему; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; контроль целостности программного обеспечения и аппаратуры; идентификация пользователей, программно-аппаратные методы аутентификации личности пользователей, парольные системы. Защита на вход в компьютерную систему средствами BIOS; настройки параметров безопасности и оптимизация ресурсов в CMOS-памяти. Защита информации на машинных носителях. Проблемы хранения данных, их содержание и причины возникновения. Логическая организация дискового пространства. Общие характеристики файловых систем с точки зрения информационной безопасности. Обеспечение защиты компьютерной информации на машинных носителях. Защищенные файловые системы. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Восстановление информации с резервных копий. Профилактика магнитных носителей и файловой системы ПЭВМ. Виды и стратегии резервирования компьютерной информации. Использование стандартных программ-архиваторов для резервирования информации. Отказоустойчивые дисковые конфигурации (RAID). Технология RAID, резервирование, кластеризация. Угрозы, связанные с возможными атаками с целью осуществления несанкционированного доступа. Организация защищенных компьютерных систем на базе ОС Windows XP. Тестирование состояния защищенности компьютерных систем от несанкционированного

		доступа. Аудит локальной системы; настройка и просмотр аудита. Область действия настроек аудита. Средства мониторинга и оптимизации рабочей станции. Предотвращение сбоев в работе в ОС.
4	Антивирусная защита компьютерных систем	Антивирусная защита компьютерных систем. Классификация и возможности вредоносных программ. Меры антивирусной профилактики и уменьшения последствий вирусных атак. Обнаружение и удаление компьютерных вирусов: методы и антивирусные средства. Признаки действия программных закладок и способы их выявления.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Комплексное обеспечение защиты информации в объектах информатизации

Печатные издания

1. Проскурин, В.Г.. Защита программ и данных : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 090900 "Информ. безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информ. Безопасность автоматизир. систем" / В. Г. Проскурин .— Москва : Академия, 2011 .— 208 с. (25 экз.)

2. Ермаков, Д.Г. Применение антивирусных программ для обеспечения информационной безопасности : учебное пособие для студентов, обучающихся по программе бакалавриата по направлениям подготовки 080500 "Бизнес-информатика", 230700 "Прикладная информатика", 080100 "Экономика" / Д. Г. Ермаков, А. В. Присяжный ; Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина .— Екатеринбург : Издательство Уральского университета, 2013 .— 64 с (5 экз.)

3. Платонов, Владимир Владимирович. Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / В. В. Платонов .— Москва : Академия, 2013— 336 с. (5 экз.)

Дополнительная литература:

1. Е.А. Степанов Информационная безопасность и защита информации : Учеб. Для студентов вузов / Е. А. Степанов, И. К. Корнеев .— Москва : ИНФРА-М, 2001 .— 304 с. (25 экз.)

2. В. А. Копылов. Информационное право : Учебник / В. А. Копылов ; Моск. гос. юрид. акад. — 2-е изд., перераб. и доп. — Москва : Юристъ, 2002 .— 512 с. ; 22 см .— (institutiones) .— Библиогр. в примеч, библиогр.: с. 506-510 (5 экз)

3. Теоретические основы компьютерной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем", "Информ. Безопасность телеком. систем" / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков .— М. : Радио и связь, 2000 (4 экз.)

4. Баранова, Е.К.. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш .— Москва : КНОРУС, 2015

Методические разработки

1. Гуляев, В.П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации : учебно-методический комплект для студентов, обучающихся по направлению 090106.65-Информационная безопасность телекоммуникационных систем / В. П. Гуляев ; Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина .— Екатеринбург : Издательство Уральского университета, 2014 .— 164 с. (5 экз.)

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.

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru
http://lib.urfu.ru/mod/data/view.php?id=1379]

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ».
http://www.edu.ru/ - Федеральный портал. Российское образование.
http://study.ustu.ru – портал информационно-образовательных ресурсов УрФУ.
http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ.

Электронные образовательные ресурсы

Не предусмотрено

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 3

Комплексное обеспечение защиты информации в объектах информатизации

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. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet* *4. Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.

		экраном. *Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.*	

ПРОГРАММА МОДУЛЯ
Защита информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 4
Методы резервирования и восстановления информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Поршнев Сергей Владимирович	д. т. н., профессор	Директор УНЦ ИБ, профессор	Учебно-научный центр «Информационная безопасность»

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 4

Методы резервирования и восстановления информации

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. Содержание дисциплины 4

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Технологии хранения данных	Технология хранения данных. Логика хранения данных. Причины потерь информации. Виды потерь информации. Защита и безопасность данных.
Р2	Стратегия защиты и восстановления данных	Обеспечение бесперебойного электропитания. Виды защитных устройств. Источники бесперебойного питания. Виды защитного программного обеспечения. Программы контроля целостности данных. Антивирусные программы. Программные средства разграничения и контроля доступа. Средства идентификации пользователей. Средства контроля действий пользователя. Средства контроля процессов. Программные средства сетевой защиты. Системы обнаружения атак. Сетевые сканеры и антиспамеры. Средства криптографической защиты
Р3	Сохранение данных при резервном копировании	Типы резервного копирования. Резервное копирование файлов и образов. Резервное копирование по плану. Полное, дифференциальное и инкрементное резервное копирование. Резервное копирование с агентами и без них. Выбор решений для резервного копирования.
Р4	Безопасное хранение резервных копий	Настройка политики хранения данных. Выбор ПО, оборудования и сайтов. Сжатие и дедупликация данных. Оценка стоимости хранения.
Р5	Технологии резервного копирования данных	Архивация и резервное копирование. Методы резервного копирования. Средства резервного копирования. Устройства хранения данных. Технология RAID. Программы для резервного копирования. Программы архивации данных.
Р6	Управление резервным копированием	Возможности резервного копирования. Оптимальный план восстановления и проверка его эффективности. Отслеживание исполнения плана резервирования данных. Настройка окна резервного копирования.
Р7	Настройка системных параметров резервирования и восстановления информации	Установка параметров BIOS. Основные функции BIOS. Параметры загрузки системы. Установка параметров файловой системы. Организация хранения данных на жестком диске. Логическая структура жесткого диска. Хранение данных в файловой системе FAT32.

		Хранение данных в файловой системе NTFS. Конфигурирование логических дисков. Монтирование дисков. Инструменты для работы с разделами дисков. Копирование разделов. Создание резервного раздела. Конвертирование разделов. Обслуживание дисков. Дефрагментация диска. Средства дефрагментации Windows и сторонних производителей. Профилактика аппаратных сбоев и отказов. Настройка интерфейса файловой системы.
P8	Восстановление системной информации	Восстановление BIOS. Коррекция параметров BIOS. Установка параметров BIOS по умолчанию. Перезапись BIOS. Устранение проблем с загрузкой системы, файлами управления загрузкой и драйверами устройств. Средства восстановления Windows. Меню режимов загрузки Windows. Восстановление системы и создание новой точки восстановления. Программа проверки и восстановления системных файлов. Восстановление системного реестра. Описание реестра Windows. Средства восстановления реестра Windows. Программы для работы с реестром от сторонних разработчиков
P9	Восстановление данных пользователя системы	Общие правила восстановления данных. Выбор программных средств восстановления. Восстановление данных на жестком диске. Восстановление данных на сменных носителях.
P10	Восстановление данных на жестких дисках	Восстановление логической структуры диска. Восстановление главной загрузочной записи. Восстановление удаленных и «потерянных» разделов. Восстановление данных в файловой системе NTFS. Восстановление элемента таблицы разделов. Восстановление загрузочного сектора раздела NTFS. Восстановление служебной информации в MFT

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 4

Методы резервирования и восстановления информации

Печатные издания

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. 70 экз

Дополнительная литература:

Бигелоу, Стивен Дж. Сети: поиск неисправностей, поддержка и восстановление / С. Дж. Бигелоу ; [пер. с англ. Ю. Гороховского] .— СПб. : БХВ-Петербург, 2005 .— 1200 с. : ил.

Методические разработки

Не предусмотренно

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

http://lib.urfu.ru/mod/data/view.php?id=1379]

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

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ».
http://www.edu.ru/ - Федеральный портал. Российское образование.
http://study.ustu.ru – портал информационно-образовательных ресурсов УрФУ.
http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ.

Электронные образовательные ресурсы

[*список наименований ЭОР, имеющих статус «ЭОР УрФУ», ресурсов Интернет с указанием режима доступа*]

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 4

Методы резервирования и восстановления информации

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. Реквизиты подтверждающего документа
	Лекции; Практические занятия; Консультации; Самостоятельная работа студентов;	*1. Компьютерный класс.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3.Персональные компьютеры, объединенные в сеть, имеющей выход в Интернет.* *4. Р-402, Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.* *5. Р-411. Персональные компьютеры – 15. Сервер – 1. Мультимедийный проектор с экраном.* *Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.*	1. Microsoft Windows 7 Enterprise SP1, Windows Server 2008 R2 Enterprise; 2. Microsoft Windows XP SP3, Microsoft Windows Server 2003 R2 Enterprise; 3. Microsoft Internet Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.

ПРОГРАММА МОДУЛЯ
Защита информации

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 5

Программно-аппаратные средства
защиты информации
Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Сафиуллин Н.Т.	К.т.н.	доцент	Департамент Информационных технологий и автоматики

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

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 5

Программно-аппаратные средства защиты информации

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. Содержание дисциплины 5

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
PI	Принципы Фон-Неймана и общее устройство современного компьютера.	Общее устройство и логика работы современного компьютера. Устройство управления и арифметикологическое устройство. Адреса и адресация. Линейность и однородность памяти. Двоичное кодирование. Программное управление. Регистры процессора. Счетчик команд. Программная и аппаратная организация стека. Передача управления. Регистр флагов. Режимы работы процессоров. Организация памяти в незащищенном режиме. Параграфы и сегменты. Адресация в незащищенном и защищенном режимах. Таблицы дескрипторов. Техника Родена. Начальная загрузка. BIOS. POST. Область данных BIOS. LBA. MBR. Загрузочный сектор. Блок управления памятью. Запуск и исполнение программ. Линия A20. HMA. UMA. EMM. EMS. Режим SMM. Гарвардская и принстонская архитектуры
PII	Работа с внешними устройствами	Системная шина. Внешнее устройство. Контроллер устройства. Регистры и области данных устройства. Общая схема подключения внешних устройств. Пространство ввода-вывода. Порт ввода-вывода. Отображение регистров и областей данных в оперативную память и пространство ввода-вывода. Порты-алиасы.
PIII	Механизм прерываний	Поллинг и прерывания – логика работы. Классификация прерываний. Аппаратные, программные, внешние, внутренние, маскируемые, немаскируемые, пошаговые, отладочные прерывания. Исключения и особенности их обработки. NMI и SMI. Обработчик прерывания. Контекст. Вектор прерывания. Таблица векторов прерываний. Последовательность обработчиков и правила работы обработчиков в последовательности. Резидентная программа. Мультиплексное прерывание.
PIV	Контроллер прерываний	Общая схема подключения, алгоритм и режимы работы контроллера прерываний. Подключение внешних устройств к контроллеру. Регистр запросов, регистр состояния и регистр масок. Назначение векторов прерываний устройствам. Запросы на прерывание уровнем и фронтом. Алгоритм вызова обработчика с учетом механизма приоритетов. Подключение нескольких устройств к одному уровню прерываний. Совместная работа обработчиков на одном уровне.

		Отбой контроллера и отбой устройства. Работа нескольких контроллеров в каскаде с примерами.
PV	Организация ввода-вывода	Видеопамять и видеорежимы. Структура видеопамяти. Алфавит и кодировка. Знакоместо и его адрес в памяти. Код и атрибут символа. Отображение информации в текстовых и графических режимах. Видеостраницы. Устройство клавиатуры. Скан-код символа. Работа клавиатурных драйверов. Устройство кольцевого буфера и правила работы с ним. Работа с манипулятором «мышь».
PVI	Таймеры, измерение времени и генерация звука	Системный таймер и режимы его работы. Отличие генератора частоты от генератора меандра. Схема подключения системного таймера. Алгоритм программирования и регистры каналов. Работа системного таймера с контроллером прерываний и контроллером памяти. Алгоритм генерации звука. Программируемый периферийный интерфейс. Работа с часами реального времени и CMOS. Измерение временных промежутков с использованием возможностей таймеров.
PVII	Компьютерная память	Статическая, динамическая, синхронная и асинхронная память. Регенерация памяти. Алгоритмы чтения и записи. Латентность, время доступа и время деактивации. DRAM. SDRAM. FPM. EDO. BEDO. DDR. DDR2. DDR3. SRAM. SSRAM. Энергонезависимая память. ROM. PROM. EPROM. EEPROM. FRAM. Shadow ROM. Механизмы регенерации. CBR. FLASH-память. Работа полевого транзистора с плавающим затвором. Понятие кадра. NOR. NAND. Работа микросхем SLC, MLC и X3.
PVIII	Прямой доступ к памяти	Механизм прямого доступа к памяти (DMA). Устройство и алгоритм работы контроллера DMA. Режимы работы и программирование. Схема подключения контроллера. Примеры работы устройств с использованием контроллера.
PIX	Системные шины. ISA, EISA, PCI	Системные шины и их характеристики. Пропускная способность. Протокол шины. Шина ISA. Шина адреса. Шина данных. Шина управления. BUSmastering. Распределение ресурсов. Спецификация протокола ISA PnP. Протокол изоляции. Шина EISA. Архитектура шины PCI. Адресация устройств на шине. Обработка прерываний в системе с шиной PCI. Конфигурационное пространство PCI. Мезонинная шина. Эмуляция ISA и PCI в современных чипсетах.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Электронные ресурсы (издания)

1. М. Гук, Аппаратные интерфейсы ПК Энциклопедия. СПб, «Питер», 2002. http://libarch.nmu.org.ua/handle/GenofondUA/4726
2. Intel® 64 and IA-32 architectures software developer's manual volume 1: Basic architecture https://software.intel.com/sites/default/files/managed/a4/60/253665-sdm-vol-1.pdf
3. Intel® 64 and IA-32 architectures software developer's manual volume 2A: Instruction set reference, A-L https://software.intel.com/sites/default/files/managed/ad/01/253666-sdm-

vol2a.pdf
4. Intel® 64 and IA-32 architectures software developer's manual volume 2B: Instruction set reference, M-U https://software.intel.com/sites/default/files/managed/7c/f1/253667-sdm-vol2b.pdf
5. Intel® 64 and IA-32 architectures software developer's manual volume 2C: Instruction set reference, V-Z https://software.intel.com/sites/default/files/managed/7c/f1/326018-sdm-vol-2c.pdf
6. Intel® 64 and IA-32 architectures software developer's manual volume 2D: Instruction set reference https://software.intel.com/sites/default/files/managed/7c/f1/334569-sdm-vol-2d.pdf
7. Intel® 64 and IA-32 architectures software developer's manual volume 3A: System programming guide, part 1 https://software.intel.com/sites/default/files/managed/7c/f1/253668-sdmvol-3a.pdf
8. Intel® 64 and IA-32 architectures software developer's manual volume 3B: System programming guide, part 2 https://software.intel.com/sites/default/files/managed/7c/f1/253669-sdmvol-3b.pdf
9. Intel® 64 and IA-32 architectures software developer's manual volume 3C: System programming guide, part 3 https://software.intel.com/sites/default/files/managed/7c/f1/326019-sdmvol-3c.pdf
10. Intel® 64 and IA-32 architectures software developer's manual volume 3D: System programming guide, part 4 https://software.intel.com/sites/default/files/managed/7c/f1/332831-sdmvol-3d.pdf
11. Магда, Ю.С. Программирование и отладка C/C++ приложений для микроконтроллеров ARM / Ю.С. Магда. - Москва : ДМК Пресс, 2012. - 170 с. : ил. - ISBN 978-5-94074-745-1 - URL: http://biblioclub.ru/index.php?page=book&id=245894
12. Intel® 64 and IA-32 architectures software developer's manual volume 4: Model-specific registers https://software.intel.com/sites/default/files/managed/22/0d/335592-sdm-vol-4.pdf
13. Intel® 64 and IA-32 architectures optimization reference manual https://software.intel.com/sites/default/files/managed/9e/bc/64-ia-32-architecturesoptimization-manual.pdf
14. Intel® architecture instruction set extensions programming reference https://software.intel.com/sites/default/files/managed/c5/15/architecture-instruction-setextensions-programming-reference.pdf
15. 5-Level Paging and 5-Level EPT white paper https://software.intel.com/sites/default/files/managed/2b/80/5-level_paging_white_paper.pdf
16. 6th Generation Intel® Core™ Processor Family Uncore Performance Monitoring Reference Manual https://software.intel.com/sites/default/files/managed/ea/25/334060-6th-gen-intel-coreprocessor-uncore.pdf
17. Intel® Virtualization Technology for Directed I/O architecture specification https://software.intel.com/sites/default/files/managed/c5/15/vt-directed-io-spec.pdf

Печатные издания

1. *Колесниченко, О. В. Аппаратные средства PC : энцикл. аппаратных ресурсов персонального компьютера : наиб. полн. рук. / О. В. Колесниченко, И. В. Шишигин .— 4-е изд., перераб. и доп .— Санкт-Петербург : БХВ-Петербург, 2003 .— 1006 с. : ил. ; 24 см .— (В подлиннике) .— Предм. указ.: с. 995-1004. — ISBN 5941570155*
2. *Ю.С.Лукач, Базовая система ввода-вывода, Свердловск, Инженерно-техническое бюро, 1990 Книга выдается в электронном виде с согласия автора.*
3. *Ю.С.Лукач, А.Е.Сибиряков, Архитектура ввода-вывода персональных ЭВМ, Второе издание, Свердловск, НТЦ «Форум», 1991 Книга выдается в электронном виде с согласия авторов.*

Методические разработки

Не используются.

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.

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru
http://lib.urfu.ru/mod/data/view.php?id=1379]

Базы данных, информационно-справочные и поисковые системы

Библиотека УрФУ lib.urfu.ru
Библиотека УрФУ lib.urfu.ru
Google. https://www.google.ru
Электронно-библиотечная система Издательства Лань: https://e.lanbook.com/
Library Archive National Mining University of Ukraine: http://libarch.nmu.org.ua/
Научная электронная библиотека: https://elibrary.ru

Электронные образовательные ресурсы

Не используются

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 5

Управление проектами в области информационной безопасности

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. Реквизиты подтверждающего документа
	Лекции; Лабораторные занятия; Консультации; Самостоятельная работа студентов;	*1.Лекционная аудитория, оснащенная компьютером и видеопроетором.* *2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.* *3. Класс IBM совместимых ПЭВМ.*	• *Компьютер, на котором установлено программное обеспечение: MS Excel, Project Expert 7, MS Project.*