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
«27» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
1156863

Модуль
Информационные технологии

Екатеринбург, 2021

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

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

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Информационные технологии

1.1. Аннотация содержания модуля

Модуль «Информационные технологии» обеспечивает формирование компетенций в области применения компьютерных технологий, необходимых для решения профессиональных практических задач. Студенты знакомятся с видами будущей профессиональной деятельности, приобретают понимание сущности и значения информатизации в обществе. Изучение модуля способствует формированию информационной грамотности.

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.	Безопасность веб-приложений	*5/180*
2.	Информационные технологии в области защиты информации	*3/108*
3.	Криптографические методы защиты информации	*5/180*
4.	Теория информации	*3/108*
5.	Языки и методы программирования	*10/360*
	ИТОГО по модулю:	*26/936*

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Информатика
Постреквизиты и кореквизиты модуля	-

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-7. Способен создавать программы на языках высокого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования;	"РО1-З ОПК7 Знает алгоритмические основы программирования на языках общего назначения" "РО2-З ОПК7 Знает языки программирования общего назначения" "РО3-З ОПК7 Знает методы, реализуемые в современных инструментальных средствах программирования"	"РО1-У ОПК7 Умеет осуществлять обоснованный выбор способов организации программ и инструментария программирования при решении профессиональных задач"	"РО1-В ОПК7 Имеет навыки разработки алгоритмов для последующего создания программ на языках общего назначения" "РО2-В ОПК7 Имеет навыки использования типовых инструментальных средств программирования для решения профессиональных задач"	

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
Информационные технологии

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1
Безопасность веб-приложений

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

Безопасность веб-приложений

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	Разработка сетевых приложений	Основы PHP.Формы. Работа с файловой системой. Сессии. HTTP-заголовки ответа сервера. Основы работы с базами данных Сокеты и сетевые функции Размещение Web-сайта на сервере
2	Методы оптимизации веб-приложений	Введение. Продвижение сайтов. Внутренняя поисковая оптимизация (SEO) Внешняя поисковая оптимизация (SEO) Индексация сайта Увеличение посещаемости сайта Конвертация трафика
3	Технологии обеспечения безопасности веб-приложений	Основные принципы построения безопасных сайтов Понятие безопасности приложений и классификация опасностей Источники угроз информационной безопасности и меры по их предотвращению Регламенты и методы разработки безопасных веб-приложений Безопасная аутентификация и авторизация Повышение привилегий и общая отказоустойчивость системы Проверка корректроности данных, вводимых пользователем. Публикация изображений и файлов. Методы шифрования. SQL-инекция. XSS-инъекции
4	Основы Web-технологий	Планирование, организация и проектирование web-сайта. Основы web-технологий Web-дизайн

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность веб-приложений

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. Ю. Родичева Нормативная база и стандарты в области информационной безопасности: учеб. пособие для студ. сред. проф. образования / А.В. Остроух. – 1-е изд. – М.: Издательский центр «Академия», 2015. – 208 с.

2.А.А. Борисенко Web-дизайн. Просто как дважды два. - .: Экспо, 2017 -320с.

3.К. Панфилов. По ту сторону веб-страницы. – СПб, 2015. – 440с.

4.Е.В. Михеева Информационные технологии в профессиональной деятельности: учеб. пособие для студ. сред. проф. образования / Е.В.Михеева. – 12-е изд., стер. – М.: Издательский центр «Академия», 2016. – 384 с.

5.Е.В. Михеева Практикум по информационным технологиям в профессиональной деятельности: учеб. пособие для студ. учреждений сред. проф. образования / Е.В. Михеева. – 12-е изд., стер. – М.: Издательский центр «Академия», 2016. – 256 с.

Дополнительная литература:

1.И.А. Коноплева, О.А. Хохлова, А.В. Денисов Информационные технологии: учебное пособие / под ред. И.А.Коноплевой. – 2-е изд., перераб. и доп. – М.: Проспект, 2010. – 328с.

2.Д.И. Ачисова Лекции по дисциплине «Информационные технологии». – ГОУ ВПО «Кубанский государственный университет», 2010.

3.Д.Ю. Усенков Коммуникационные технологии: практикум / Д.Ю. Усенков, О.Б. Богомолова. – М.: БИНОМ. Лаборатория знаний, 2013. – 303 с.: ил.

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

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность веб-приложений

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. Сертифицированный программно-аппаратный*	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

		комплекс межсетевого экранирования. *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	Information Services 6.0. 4. Программное обеспечение Microsoft Office версии не менее 2010.

ПРОГРАММА МОДУЛЯ
Информационные технологии

РАЗДЕЛ 3. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 2
Информационные технологии в области защиты информации

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

3. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 2

Информационные технологии в области защиты информации

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

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Концепция технической защиты информации	Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
2	Теоретические основы технической защиты информации	Информации как предмет защиты. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства, и системы как источники опасных сигналов. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения.

		Организованные каналы утечки (съема) информации – закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала.
3	Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства. Физические процессы при подавлении опасных сигналов. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Средства предотвращения утечки информации по техническим каналам. Средства 7 маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.
4	Организационные основы технической защиты информации	Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

3.3. Программа дисциплины реализуется на государственном языке Российской Федерации

3.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационные технологии в области защиты информации

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. Бузов Г.А., Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев .— М. : Горячая линия - Телеком, 2005 .— 416 с.

2. Домарев В. В. Безопасность информационных технологий. Системный подход: другое. ТИД ДС, 2004. — 992 с.

3. Технические средства и методы защиты информации. Учебное пособие для вузов/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников, А.А. Солдатов, С.В.Скрыль. Под ред. А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2009. – 616 с..

4. Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности / А. А. Торокин .— Москва : Гелиос АРВ, 2005 .— 960 с.

5. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки: учебник. РГГУ, 2002. — 400 с.

6. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности 230201 "Информ. системы и технол." / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .— Москва : Академия, 2006 .— 336 с.

Дополнительная литература:

1. Зегжда Д. П. Основы безопасности информационных систем: монография. Горячая линия-Телеком, 2000. - 452 с.

2. Андрианов, В. И. Устройства для защиты объектов и информации : Справ. пособие / В.И. Андрианов, А.В. Соколов; Под ред. С.А. Золотарева .— 2-е изд., перераб. и доп. — СПб.; М. : Полигон : АСТ, 2000 .— 256 с.

3. Андрианов В. И.; Золотарев С. А., Соколов А. В. Устройства для защиты объектов и информации: Полигон : АСТ, 2000. (1 экз. в фонде).

4. Барсуков, В. С. Современные технологии безопасности: интегральный подход / В.С. Барсуков, В.В. Водолазкий .— М. : Нолидж, 2000 .— 496 с.

5. Горохов П. К. Информационная безопасность Радио и связь, 1995. .— 224 с.

6. Петраков, А.В. Основы практической защиты информации : Учеб. пособие для вузов по спец. 20. 18. 00 "Защищенные системы связи" / А.В. Петраков .— 2-е изд. — М. : Радио и связь, 2000 .— 368 с.

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

5. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
6. http://www.edu.ru/ - Федеральный портал. Российское образование.

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

3.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

*Информационные технологии в области защиты 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. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	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
Информационные технологии

РАЗДЕЛ 4. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 3
Криптографические методы защиты информации

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

4. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 3

Криптографические методы защиты информации

4.1. 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);*

4.2. Содержание дисциплины 3

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Общие принципы криптографии	История криптологии. Классификация методов шифрования информации. Шифры замены. Шифры перестановки. Блочные шифры. Шифры гаммирования. Поточные шифры. Модели шифров по К. Шеннону. Математические основы криптографии. Принципы построения и свойства генераторов псевдослучайных последовательностей
2	Симметричные криптографические системы	Блочные и поточные шифры. Криптосистемы Фейстеля. Американский стандарт шифрования данных DES, основные режимы работы алгоритма. Алгоритм IDEA. Стандарт AES. Стандарт шифрования ГОСТ Р 34.12-2015, режимы работы. Задача криптоанализа. Криптоанализ “полным перебором”. Разностный криптоанализ. Линейный криптоанализ.
3	Асимметричные криптографические системы	Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Схема шифрования Эль Гамаля. Проблема аутентификации данных и электронная цифровая подпись. Хеш-функции: SHA, на основе симметричных блочных криптоалгоритмов, ГОСТ. Схемы создания и проверки цифровой подписи с помощью несимметричных схем шифрования. Протоколы электронной цифровой подписи (ЭЦП). Классификация атак на схемы ЭЦП.
4	Управление криптографическими ключами	Криптографические протоколы. Протоколы организации защищенного обмена информацией с подтверждением подлинности участников при наличии прямого защищенного канала без посредника и с использованием посредника. Разрядность ключа. Генерация ключей. Хранение ключей. Схемы распределения ключей. Время жизни ключа. Создание секретного ключа с обменом через незащищенный канал.

4.3. Программа дисциплины реализуется на государственном языке Российской Федерации

4.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

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. Основы криптографии : учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин .— 3-е изд., испр. и доп. — М. : Гелиос АРВ, 2005 .— 480 с. 25 экз

2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов .— М. : КУДИЦ-ОБРАЗ, 2001 .— 368 с.

Дополнительная литература:

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф. Шаньгина .— М. : Радио и связь, 1999 .— 328 с. 24 экз

2. Осипян В.О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян .— М. : Гелиос АРВ, 2004 .— 144 с. 11 экз

3. Нечаев В.И. Элементы криптографии. (Основы теории защиты информации : Учеб. пособие для вузов / Под ред. В.А. Садовничего .— М. : Высш. шк., 1999 .— 109 с.

4. Молдовян А.А. Криптография / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов .— СПб. : Лань, 2001 .— 224 с.

5. Баричев С. Г. Основы современной криптографии : Учеб. курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов .— 2-е изд., испр. и доп. — М. : Горячая линия-Телеком, 2002 .— 175 с.

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

4.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические методы защиты 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. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	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
Информационные технологии

РАЗДЕЛ 5. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 4
Теория информации

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

5. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 4

Теория информации

5.1. 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);*

5.2. Содержание дисциплины 4

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Понятие информации, энтропии. Системы связи. Дискретные источники.	Понятие информации, энтропии. Системы связи. Дискретные источники. Описание источника при помощи случайного процесса. Статистическая независимость. Марковские источники. Эргодичность. Эргодичность бернуллиевского источника. Вывод формулы энтропии (по Фадееву). Свойства энтропии. Теорема о максимальном значении энтропии. Энтропия в единицу времени источника сообщений.
2	Взаимная информация и её свойства.	Взаимная информация и её свойства.
3	Задача кодирования дискретного источника кодами равной длины.	Задача кодирования дискретного источника кодами равной длины. Постановка задачи. Понятие скорости кодирования. Высоковероятные множества и их свойства. Прямая и обратная теоремы кодирования Шеннона дискретного источника кодами равной длины.
4	Задача кодирования дискретного источника кодами неравной длины. Сжатие информации.	Задача кодирования дискретного источника кодами неравной длины. Постановка задачи. Стоимость кодирования. Свойство однозначной дешифрируемости кода. Префиксные коды. Необходимое и достаточное условие однозначной дешифрируемости кода. Разрешимость задачи определения однозначной дешифрируемости. Полные коды. Теорема кодирования дискретного источника кодами неравной длины. Алгоритмы построения оптимальных кодов (Фано, Шеннона, Хаффмена). Арифметическое кодирование. Словарные методы сжатия информации. Построение бинарного оптимального кода при равновероятном распределении входных вероятностей. Приложение результатов теории информации при доказательстве нижних и верхних оценок сложности реализации булевых функций в некоторых классах управляющих систем. Метод построения оптимального кода при условии, что неизвестно распределение вероятностей букв источника.
5	Дискретные каналы и их	Дискретные каналы и их свойства. Дискретный

	свойства. Скорость передачи информации в канале. Пропускная способность канала. Прямая теорема кодирования Шеннона для канала без памяти. Обращение теоремы кодирования Шеннона.	канал без памяти. Двоичный симметричный канал. Скорость передачи информации в канале. Пропускная способность канала. Расширенный канал и его пропускная способность. Решающие схемы и группировки наблюдений. Вероятность ошибочной передачи информации. Прямая теорема кодирования Шеннона для канала без памяти. Неравенство Фано. Теорема обработки информации. Обращение теоремы кодирования Шеннона.
6	Теория помехоустойчивого кодирования	Теория помехоустойчивого кодирования. Понятие помехоустойчивого кодирования. Критерий максимального правдоподобия. Кодовое расстояние. Коды с проверкой на четность. Порождающая и проверочная матрицы. Синдром. Алгоритм декодирования для кодов с проверкой на четность. Линейные коды и алгоритм их декодирования. Граница Хэмминга. Код Хэмминга. Циклические коды. Кодирование и декодирование циклических кодов.

5.3. Программа дисциплины реализуется на государственном языке Российской Федерации

5.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория информации

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. Основы теории информации: Учебное пособие / А.М. Маскаева. - М.: Форум: НИЦ ИНФРА-М, 2014. - 96 с.: 70x100 1/16. (обложка) ISBN 978-5-91134-825-0, 500 http://znanium.com/bookread.php?book=429571

2. Чикрин Д. Е. Теория информации и кодирования: курс лекций. Казанский (Приволжский) федеральный университет: Высшая школа информационных технологий и информационных систем, Кафедра автономных робототехнических систем, 2013 http://libweb.ksu.ru/ebooks/50-ITIS/50_000337.pdf

3. Чепкунова Е. Г. Пособие для подготовки к экзамену по дисциплине "Теоретические основы информатики". Раздел "Кодирование информации": [учебное пособие]. Казанский (Приволжский) федеральный университет: Институт вычислительной математики и информационных технологий, Кафедра математики и вычислительных технологий, 2012 http://libweb.ksu.ru/ebooks/09-IVMIT/09_150_2012_000118.pdf

Дополнительная литература:

1. Введение в дискретную математику : Учеб. пособие для студентов вузов, обучающихся по спец. "Прикладная математика" / С.В.Яблонский .? 3-е изд., стер. ? М. : Высш. шк., 2002 .? 384с.

2. Задачи по дискретной математике для контрольных и самостоятельных работ. О.-д.

функции. Теория кодирования. Графы [Текст: электронный ресурс] : учебный практикум / Казан. гос. ун-т ; сост.: А. В. Васильев, д.ф.-м.н., проф. Н. К. Замов, к.ф.-м.н., доц. П. В. Пшеничный .? Электронные данные (1 файл: 0,23 Мб) .? (Казань : Казанский государственный университет, 2009)

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

5.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория 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. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	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
Информационные технологии

РАЗДЕЛ 6. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 5
Языки и методы программирования

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

6. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 5

Языки и методы программирования

6.1. 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);*

6.2. Содержание дисциплины 5

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Введение	Основные этапы решения задач на ЭВМ. Понятие о среде разработки. Программа как формализованное описание процесса. Технология программирования и основные этапы ее развития. Проблемы разработки сложных программных систем. Жизненный цикл программного средства. Модели разработки: каскадная, с промежуточным контролем, спиральная и т.д.; CASE и RAD-технологии. Язык UML. Принципы применения, основные артефакты и диа- 5 граммы. Определение требований к программному средству. Функциональная спецификация программного средства. Методы контроля внешнего описания программного средства. Понятие качества программного средства. Контроль в процессе разработки ПС. Понятие ошибки в программном средстве. Надежность программного средства. Обеспечение надежности ПС.
2	Архитектура ПО. Методы проектирования	Понятие архитектуры программного средства. Виды архитектур программных средств. Способы конструирования программ. Диалоговые программы. Модульные программы. Монолитные, двух- и трехуровневые архитектуры
3	Технология создания программного кода. Язык C#	1. Основные элементы языка. Используемые символы. Константы и идентификаторы. Ключевые слова. Комментарии 2. Типы данных, литералы и переменные. Категории типов данных. Типы-значения. Целые, плавающие, десятичные, логический, перечислимый тип. Литералы. Массивы. Динамические структуры данных. Классы. Инициализация. Примеры встроенных классов. Строки. Списки, словари, хэш-таблицы, очереди. Область определения. Преобразование типов. 3. Управляющие операторы. Категории операторов. Пустой оператор. Составной оператор. Условные операторы if и switch.

		Операторы цикла (for,while,do while). Операторы перехода (break, continue, return, goto). 4. Операции и выражения. Виды и арность операций. Преобразования при вычислении выражений. Мультипликативные операции. Аддитивные операции. Операции сдвига. Поразрядные операции. Логические операции. Операция последовательного вычисления. Инкремент, декремент. Условная операция. Присваивание. Приоритеты операций и порядок вычислений. Скобки. Оператор «?». 5. Методы. Понятие метода. Возвращаемое значение и аргументы. Функции с переменным числом аргументов. Аргументы по умолчанию. Именованные аргументы. Необязательные аргументы. Полиморфизм. Перегрузка. Статические методы и методы экземпляра. Методырасширения. Рекурсия. Использование переменных. Некоторые библиотечные методы. 6. Классы. Инкапсуляция. Определение класса. Создание объектов. Класс как переменная ссылочного типа. Присваивание. Конструкторы. Сборка мусора и деструкторы. Ключевое слово this. Управление доступом. Использование ref/out. Статические классы. Индексаторы и свойства. 7. Наследование. Реализация наследования. Создание иерархии классов. Порядок вызова конструкторов. Ссылка на базовый класс. Абстрактные классы. Виртуальные методы и их переопределение. Класс object. Предотвращение наследования. Упаковка и распаковка, object. 8. Массивы и структуры данных. Основы работы со структурами. Структуры и функции. Многомерные массивы. Массивы структур. Структуры со ссылками на себя: бинарные деревья, списки. Определение новых типов. 9. Интерфейсы. Реализация. Составляющие интерфейса. Наследование. Случаи применения интерфейса. Стандартные интерфейсы. 10. Обработка исключительных ситуаций. Специфика обработки ошибок в C#. Класс System.Exception. Применение try, catch и finally. Перехват всех и некоторых 6 исключений. Последовательность блоков catch. Вложение блоков. Ручная генерация исключений. Создание собственных типов исключений. 11. Применение средств ввода-вывода и обработки данных. Ввод, вывод и редактирование информации с использованием стандартных библиотек. Потоки. Консоль. Организация ввода-вывода информации с использованием внешних файлов. XML.Общий обзор методов ввода, вывода и обработки информации. Регулярные выражения. 12.

		Делегаты, события и лямбда-выражения. Делегаты. Анонимные методы. События. Лямбда-выражения. Основы C# LINQ. 13. Структура программы. Структура программы. Библиотеки. Блоки программы. Объявление переменных. Классы и их взаимодействие. Пространства имен. 14. Создание цельных приложений. Консольные приложения. Оконные приложения. Проектирование интерфейса. Диалог с пользователем.
4	Работа с базами данных в C#	Технология ADO.Net. Работа с базой данных Access. Вывод результатов запросов к базе данных на форму. Язык LINQ. Работа с локальными наборами данных. Работа с базой данных MS SQL
5	Коллективная разработка ПО	Обзор и классификация средств поддержки коллективной разработки ПО. Программные средства планирования и управления процессом разработки. Графики и диаграммы рабочего процесса. Истории пользователя. Этапы и задачи. Применение систем управления документами. Системы контроля версий. CASE-технологии.
6	Тестирование и отладка ПО	Категории программных ошибок. Типы тестов. Тестирование на этапе планирования. Тестирование на этапе проектирования. Тестирование "белого ящика" на стадии кодирования. Регрессионное тестирование. Тестирование "черного ящика". Разработка тестов. Модульное тестирование. Mock-объекты. Изоляция модулей программы. Тестирование на основе поведения. Интеграция тестирования в процесс разработки.
7	Документирование, оценка качества и сопровождение ПО	Документация, создаваемая в процессе разработки программных средств. ЕСПД. Пользовательская документация программных средств. Документация по сопровождению программных средств. Стандарт ISO 9126. Модель качества. Характеристики и субхарактеристики качества программного средства. Метрики качества программного средства. Оценивание характеристик качества программных средств. Понятие сопровождения ПО. Общие рекомендации.

6.3. Программа дисциплины реализуется на государственном языке Российской Федерации

6.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Языки и методы программирования

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. Осипов, Сергей Иванович. Компьютерные науки. Основы процедурного программирования на C и C++ : учебное пособие для студентов, обучающихся по программе бакалавриата по направлению подготовки 010800 "Механика и математическое моделирование" / С. И. Осипов ; М-во образования и науки РФ, Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина, Ин-т мат. и компьют. наук. — Екатеринбург : Издательство Уральского университета, 2013. — 155 24 экз. 11

2. Гросс, Кристиан. C# 2008 и платформа .NET 3.5 Framework: Вводный курс / Кристиан Гросс ; [пер. с англ. и ред. В. А. Коваленко] .— 2-е изд. — Москва ; Санкт-Петербург ; Киев : Вильямс, 2009 .— 480 с.

3. Рихтер, Джеффри. Windows via C/C++. Программирование на языке Visual C++ : [пер. с англ.] / Д. Рихтер, К. Назар. — [М.] ; СПб. [и др.] : Русская Редакция : Питер, 2009. — 878 с. : ил. — (Мастер-класс). — ISBN 978-5-7502-0367-3. — ISBN 978-5-388-00205-1. 30 экз.

Дополнительная литература:

1. Хортон, Айвор. Visual C++ 2005 : базовый курс / Айвор Хортон ; [пер. с англ. Ю. И. Корниенко, Н. А. Мухина]. — М. [и др.] : Диалектика : [Вильямс], 2007. — 1143 с. : ил., табл. — (Программистам от программистов). — Предм. указ.: с. 1135-1143. — ISBN 978-5-8459-1016-5. 3 экз.

2. Павловская Т.А. С++. Программирование на языке высокого уровня. – СПб: Питер, 2005. – 461 с. 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

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

6.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Языки и методы программирования

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. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.* *4. Общесистемное и прикладное программное обеспечение, средства защиты информации:*	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.