МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ
МЕТОДОЛОГИЯ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Перечень сведений о рабочей программе модуля	Учетные данные
Модуль Информационная безопасность	**Код модуля** Б 1.10
Образовательная программа Информационно-аналитические системы безопасности	**Код ОП** 10.05.04/01.01
Направление подготовки Информационно-аналитические системы безопасности	**Код направления и уровня подготовки** 10.05.04
Уровень образования высшее образование - специалитет	
ФГОС ВО **10.05.04 -** Информационно-аналитические системы безопасности	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 01 декабря 2016 г., №1514

Екатеринбург, 2017

Программа модуля составлена авторами:

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

Руководитель модуля

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий
Председатель учебно-методического совета Н.В. Папуловская

Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль **С.В. Поршнев**

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

1.1. Объем модуля, 21 з.е.

1.2. Аннотация содержания модуля

В модуле изучаются следующие дисциплины: «Безопасность операционных систем», «Криптографические методы защиты информации», «Организационное и правовое обеспечение защиты информации», «Программно-аппаратные средства защиты информации» и «Техническая защита информации». Модуль направлен на формирование способности демонстрировать и применять базовые математические, естественнонаучные, гуманитарные, социально-экономические и технические знания в междисциплинарном контексте для решения инженерных задач в профессиональной области.

Результатом обучения в рамках модуля является формирование у студента следующих компетенций: способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах, способность разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности.

− способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
− способностью применять в профессиональной деятельности языки и системы программирования, инструментальные средства разработки программного обеспечения, современные методы и технологии программирования (ОПК-4);
− способность разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности (ПК-11);
− способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15).

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего			Час.	Зач. ед.
1.	(Б) Безопасность операционных систем	9	34	-	34	68	76	экзамен	144	4
2.	(Б) Криптографические методы защиты информации	7	17	-	34	51	57	зачет	108	3
3.	(Б) Организационное и правовое обеспечение защиты информации	5	34	34	-	68	76	экзамен	144	4
4.	(Б) Программно-аппаратные средства защиты информации	8	34	-	34	68	76	экзамен	144	4
5.	(Б) Техническая защита информации	7	34	-	34	68	76	экзамен	144	4
6.	(Б) Проект по модулю «Информационная безопасность»	9						Зачет по модулю		2
Всего на освоение модуля			153	34	136	323	433		756	21

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	Организационное и правовое обеспечение защиты информации, Криптографические методы защиты информации, Техническая защита информации
3.2.	**Кореквизиты**	Безопасность операционных систем, Программно-аппаратные средства защиты информации, Проект по модулю «Информационная безопасность»

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

4.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	**Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля**	**Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля**
РО-2	*Способность демонстрировать и применять базовые математические, естественнонаучные, гуманитарные, социально-экономические и технические знания в междисциплинарном контексте для решения инженерных задач в профессиональной области*	− способностью анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности (ОПК-1); − способностью применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7).
РО- 4	Способность планировать, проводить исследование и разработку мероприятий по проектам в различных отраслях экономики, осуществлять подготовку презентаций и защиту результатов исследования в рамках научно-исследовательской деятельности	− способность применять современные методы научных исследований с использованием компьютерных технологий, в том числе в работе над междисциплинарными проектами (ПК-4); − способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5); − способность готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований (ПК-6);
РО-5	*Способность применять методы, средства и технологии проектирования информационно-аналитических систем, ~~и~~ разрабатывать защитные механизмы и средства обеспечения информационной безопасности в рамках проектной деятельности*	− способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9); − способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10); − способность разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности (ПК-11); − способность разрабатывать программное и иные виды обеспечения специальных ИАС (ПК-12); − способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-13).
РО-6	*Способность применять информационно-*	− способность использовать специальные ИАС для решения задач в сфере

	аналитические системы и предпринимать меры и средства обеспечения информационной безопасности в рамках в эксплуатационно-технологической деятельности	профессиональной деятельности (ПК-14); − способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15).
РО-7	*Способность организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели в рамках организационно-управленческой деятельности*	− способность разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности (ПК-16); − способность организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-17).

4.2.Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля	Безопасность операционных систем	Криптографические методы защиты информации	Организационное и правовое обеспечение защиты информации	Программно-аппаратные средства защиты информации	Техническая защита информации	Проект по модулю
ОПК-1	*			*	*	*
ОПК-7	*	*	*	*	*	*
ПК-9	*			*	*	*
ПК-10	*			*	*	*
ПК-11	*			*	*	*
ПК-12	*			*	*	*
ПК-13	*				*	*
ПК-14		*	*		*	*
ПК-15			*		*	*
ПК-16			*			*
ПК-17			*			*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю: [*указать коэффициент, утвержденный ученым(и) советом(ами) института(ов), в котором(ых) реализуется модуль, протокол заседания ученого совета №* _____ *от* _____ *г.*]

5.2. Форма промежуточной аттестации по модулю:

[*указать форму промежуточной аттестации для оценки интегрированного результата освоения дисциплин модуля: интегрированный экзамен по модулю, выполнение и защита проекта по модулю*]

5.3. Фонд оценочных средств для проведения промежуточной аттестации по модулю (Приложение 1)

ПРИЛОЖЕНИЕ 1
к рабочей программе модуля

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

Система критериев оценивания результатов обучения в рамках модуля опирается на три уровня освоения: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю

Не предусмотрено

5.3.2.2. **Перечень примерных тем итоговых проектов по модулю**

Разработка системы защиты информации;

Разработка системы криптографической защиты информации;

Разработка программно-аппаратного комплекса контроля за проникновением в систему;

Разработка системы защиты от проникновения на уровне операционной системы;

Разработка мероприятий организационно-правого порядка по предотвращению утечки информации

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль **Информационная безопасность**	**Код модуля** **№ 1140576/33630** **УП 6938**
Образовательная программа **Информационная безопасность информационно-аналитических систем**	**Код ОП** **10.05.04/01.01**
Траектория образовательной программы (ТОП)	**Не предусмотрена**
Направление подготовки **Информационная безопасность информационно-аналитических систем**	**Код направления и уровня подготовки** **10.05.04**
Уровень подготовки **специалист**	
ФГОС ВО **Информационная безопасность информационно-аналитических систем**	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** **№ 1514 1 декабря 2016 г.**

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Авдеев Денис Викторович	-	Ст. преп.	Департамент радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Председатель учебно-методического совета В.Г. Коберниченко
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению основ криптографических методов обеспечения информационной безопасности в вычислительных системах и компьютерных сетях. Рассматриваются криптографические протоколы, алгоритмы электронной цифровой подписи, вопросы надежности криптосистем.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- –способностью применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7).
- способность использовать специальные ИАС для решения задач в сфере профессиональной деятельности (ПК-14);

В результате освоения дисциплины студент должен:

Знать:

- основные понятия криптографии,
- симметричные и асимметричные алгоритмы криптографических преобразований,
- алгоритмы цифровой подписи,
- основные криптографические протоколы,
- отечественные и международные стандарты в области криптографической защиты информации в телекоммуникационных системах.

Уметь:

- использовать стандартные криптографические алгоритмы и протоколы,
- использовать типовые методы криптоанализа,
- разрабатывать модели информационной безопасности телекоммуникационных систем,
- правильно создать ключи для криптографической защиты программных систем и данных от несанкционированного использования (доступа, копирования) или нарушения технологии работы,
- выбрать наиболее удачный криптографический протокол для защиты телекоммуникационной системы от несанкционированного доступа.

Владеть (демонстрировать навыки и опыт деятельности):

- программными и аппаратными средствами криптографической защиты информации и персональных данных,
- навыками оценки и повышения надежности криптографических систем.

1.4. Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*7*
1.	**Аудиторные занятия**	51	51	51
2.	Лекции	17	17	17
3.	Практические занятия	0	0	0
4.	Лабораторные работы	34	34	34
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	76	10,20	76
6.	**Промежуточная аттестация**	З	0,33	З, 4
7.	**Общий объем по учебному плану, час.**	108	61,53	108
8.	**Общий объем по учебному плану, з.е.**	3		3

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 11
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																					
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)										Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Общие принципы криптографии	**15**	**11**	3		8		**4**	2		2		**3**	1														
2	Симметричные криптографические системы	**17**	**13**	5		8		**4**	2		2		**12**	1				1										
3	Асимметричные криптографические системы	**13**	**9**	5		4		**4**	2		2		**3**	1														
4	Управление криптографическими ключами	**24**	**18**	4		14		**6**	2		4		**22**	1					1									
	Всего (час), без учета промежуточной аттестации**:**	**104**	**51**	**17**	**0**	**34**	**53**	**18**	**8**	**0**	**10**	**0**	**40**	**14**	**0**	**0**	**0**	**8**	**18**	**0**	**0**	**0**	**0**	**0**	**0**	**0**				
	Всего по дисциплине (час.):	**108**	**51**				**57**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Математические основы криптографии	8
2	2	Настройка протокола IPsec	8
3	3	Применение пакета PGP	4
4	4	Использование цифровых сертификатов	14
		Всего:	**34**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Изучение шифров перестановки, простой и сложной замены;*
- *Алгоритмы RSA, Диффи-Хелмана;*
- *Математические основы и алгоритмы ЭЦП;*
- *Схемы генерации ключей.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

- *Линейные и нелинейные конгруэнтные генераторы*

4.3.6. Примерный перечень тем расчетно-графических работ

- *Шифрование по алгоритму S-DES*

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.4.1. Примерная тематика контрольных работ

Не предусмотрено

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Общие принципы криптографии				*								
Симметричные криптографические системы					*			*				
Асимметричные криптографические системы				*				*				
Управление криптографическими ключами					*			*				

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

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.

9.1.2.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.

9.2. Методические разработки

1. Спиричева Н.Р. Алгоритмы блочной криптографии. ЭОР УрФУ, АПИ, 2013. Метаданные ресурса №13170

9.3. Программное обеспечение

GPG, IPsec, веб-браузер

9.4. Базы данных, информационно-справочные и поисковые системы

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

9.5. Электронные образовательные ресурсы

1. Зональная научная библиотека УрФУ — http://lib.urfu.ru
2. Портал информационно-образовательных ресурсов УрФУ — http://study.ustu.ru ;
3. Официальный сайт ИРИТ-РтФ — http://rtf.ustu.ru ;

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,4**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*7,1-7*	*25*
Домашняя работа №2	*7,1-7*	*25*
Домашняя работа №3	*7,1-7*	*25*
Домашняя работа №4	*7,1-7*	*25*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,6		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Расчетная работа	*7,8-15*	*20*
Расчетно-графическая работа	*7,8-15*	*20*
Выполнение лабораторных работ	*7,8-15*	*60*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1,0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий *Не предусмотрено*

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

1.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Место криптографии в защите информации. Физическая защита. Стеганография. Криптография.
2. Предмет криптографии. Математические основы.
3. История криптографии. Шифр Цезаря. Сцитала. Маршрутная перестановка. Квадрат Полибия.
4. История криптографии. Магический квадрат. Таблица Тритемия. Решетка Кардано.
5. История криптографии. Шифр Виженера. Шифр Плейфера. Принцип Керкгоффса.
6. История криптографии. Лента Вернама. Энигма.
7. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: математическая структура секретных систем.
8. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: теоретическая секретность.
9. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: практическая секретность.
10. Симметричная криптография. Криптоанализ простым перебором. Общая схема симметричной системы. Алгоритм S-DES.
11. Симметричная криптография. Сеть Файстеля. Алгоритм DES.
12. Симметричная криптография. Блочные шифры. Диффузия и конфузия. Проектирование S-блоков.
13. Симметричная криптография. Алгоритмы 3DES, ГОСТ 34.12-2015. Режимы использования блочных шифров.
14. Симметричная криптография. Алгоритм AES.
15. Симметричная криптография. Криптоанализ. Атаки на реализацию. Линейный криптоанализ.
16. Симметричная криптография. Квантовый криптоанализ. Производительность AES.
17. Асимметричная криптография. Проблемы традиционной криптографии. Общая схема асимметричной системы. Возможности и условия применения.
18. Асимметричная криптография. Одностороняя функция с лазейкой. Криптоанализ. Алгоритм RSA.

19. Асимметричная криптография. Протокол Диффи-Хеллмана.
20. Асимметричная криптография. Схема Эль-Гамаля. Эллиптическая криптография.
21. Совместное использование традиционной и асимметричной криптографии. Обеспечение конфиденциальности и целостности. Контроль ошибок.
22. Совместное использование традиционной и асимметричной криптографии. Имитовставка.
23. Функция хэширования. Схемы применения. Требования. Атаки. Способы построения.
24. Цифровая подпись. Назначение. Схемы применения. Атаки. Алгоритм DSA.
25. Распределение ключей. Сравнение особенностей симметричной и асимметричной систем. Иерархия ключей.
26. Распределение ключей. Сеансовые ключи. Сценарии обмена.
27. Распределение ключей. Обмен открытыми ключами. Сценарии.
28. Распределение ключей. Сертификаты открытых ключей. Сценарии обмена.
29. Средства криптографической защиты информации. IPSec.
30. Средства криптографической защиты информации. Организация иерархии удостоверяющих центров.
31. Средства криптографической защиты информации. Kerberos.
32. Распределение ключей. Удостоверяющий центр.
33. Распределение ключей. Взаимодействие УЦ. Жизненный цикл сертификата.
34. Стеганография. Современные подходы. Стегоанализ.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль **Информационная безопасность**	**Код модуля** **№ 1140576/33630** **УП 6938**
Образовательная программа **Информационная безопасность информационно-аналитических систем**	**Код ОП** **10.05.04/01.01**
Траектория образовательной программы (ТОП)	**Не предусмотрена**
Направление подготовки **Информационная безопасность информационно-аналитических систем**	**Код направления и уровня подготовки** **10.05.04**
Уровень подготовки **специалист**	
ФГОС ВО **Информационная безопасность информационно-аналитических систем**	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** **№ 1514 1 декабря 2016 г.**

Екатеринбург, 17

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Челноков Владислав Валерьевич	к.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам. председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль С.В. Поршнев

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ »

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению способов ведения разведки техническими средствами по перехвату информации, циркулирующей в объектах информатизации, принципов построения и характеристиках современных и перспективных средствах технических разведок. Изучаются критерии перехвата информации различными видами средств технических разведок, оценки возможностей аппаратуры средств технических разведок и способы определения зон разведдоступности технических разведок по получению информации о конкретных объектах, входящих в круг интересов этих разведок, рассматриваются вопросы противодействия различным видам технических разведок.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способностью применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7).
- способность использовать специальные ИАС для решения задач в сфере профессиональной деятельности (ПК-14);
- способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15).
- способность разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности (ПК-16);
- способность организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-17).

В результате освоения дисциплины студент должен:

Знать

- понятия в сфере ИБ РФ;
- цели и задачи государственной политики в сфере ИБ;
- угрозы ИБ Российская Федерация;
- законодательную базу обеспечения ИБ;
- разделение информации по категориям доступа, понятие и виды информации ограниченного доступа;
- ответственность за нарушение защиты информации ограниченного доступа
- понятие государственной тайны (ГТ);
- порядок отнесения сведений к ГТ;
- ограничения, связанные с ГТ;
- виды информации ограниченного распространения;
- требования к организаторам распространения информации в сети «Интернет»;
- процедуры ограничения доступа к интернет-ресурсам;
- меры по обеспечению доступа к информации о деятельности государственных органов и органов местного самоуправления;
- понятие интеллектуальной собственности;
- понятие программ для ЭВМ и баз данных как объектов авторского права;
- виды ответственности за нарушение авторского права;

–условия правомерного использования программ для ЭВМ и баз данных;
–понятие лицензии их видов в сфере ИБ;
–понятие сертификации;
–полномочия государственных органов по лицензированию и сертификации;
–виды сертификатов и сертифицируемых средств в сфере ИБ;
–роли компьютерных систем в преступной деятельности;
–понятие компьютерной информации;
–признаки преступлений в сфере компьютерной информации;
–принципы организации ЗИ в учреждении, предприятии;
–основы организации охраны и внутриобъектового режима;
–способы выявления инцидентов ИБ;
–виды сотрудничества с правоохранительными органами в сфере ИБ;
–обязанности и права оператора ПДн;
–государственные органы, уполномоченные осуществлять контроль и надзор за выполнением мер по обеспечению безопасности ПДн;
–ответственность за правонарушения (преступления) в сфере защиты ПДн;

Уметь:
–понимать интересы государства сфере ИБ;
–организовывать деятельность по обеспечению ИБ в соответствии с государственной политикой;
–понимать содержание нормативных правовых актов в сфере ИБ;
–организовывать деятельность по обеспечению ИБ в соответствии с нормативными правовыми актами;
–понимать содержание нормативных требований по защите ГТ;
–организовывать деятельность по защите ГТ в соответствии с нормативными правовыми актами;
–понимать содержание нормативных правовых актов в сфере ИБ;
–организовывать деятельность по обеспечению ИБ в соответствии с нормативными правовыми актами;
–понимать содержание нормативных правовых актов по охране интеллектуальной собственности;
–правомерно использовать объекты авторского права в деятельности по обеспечению ИБ;
–понимать содержание требований по лицензированию и сертификации в сфере ИБ ;
–организовывать деятельность по обеспечению ИБ с учетом требований по лицензированию и сертификации в данной сфере;
–понимать уголовно-правовые запреты в сфере ИБ ;
–выявлять признаки преступных деяний в сфере компьютерной информации;
–планировать организационные меры ИБ в соответствии с компетенцией;
–реагировать на инциденты ИБ;
–определять уровень защищенности ПДн в организации;
–планировать меры, по обеспечению безопасности ПДн в соответствии с уровнем их защищенности;
–оценивать возможности технических разведок в отношении конкретного объекта информатизации.

Владеть (демонстрировать навыки и опыт деятельности):
–методами выявления нарушения безопасности системы;
–методикой организации хранения и систематизации конфидециальной документации с учётом требований законодательства РФ.
–методами обеспечения защиты персональных данных;
–принципы и условиями обработки ПДн.

1.4. Объем дисциплины

Очная форма обучения (учебный план № 6028, в. 3)

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*5*
1.	**Аудиторные занятия**	68	68	68
2.	Лекции	34	34	34
3.	Практические занятия	17	17	17
4.	Лабораторные работы	17	17	17
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	57	7,25	57
6.	**Промежуточная аттестация**	Э	5,25	Э, 4
7.	**Общий объем по учебному плану, час.**	144	80,5	144
8.	**Общий объем по учебному плану, з.е.**	4		4

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Основные положения государственной политики в сфере обеспечения информационной безопасности (ИБ) РФ**	Основы и содержание информационной безопасности; субъекты и объекты правоотношений в сфере ее обеспечения. Доктрина информационной безопасности РФ. Национальные интересы РФ в информационной сфере и их обеспечение. Виды и источники угроз информационной безопасности РФ.
2	**Принципы правового регулирования отношений и основные понятия в сфере информации, информационных технологий и защиты информации. Ограничение доступа к информации**	Конституционные гарантии интересов личности в информационной сфере. Законодательная база обеспечения ИБ. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты: коммерческая тайна, банковская тайна, налоговая тайна, тайна связи, врачебная тайна.

		Ответственность за нарушение защиты информации ограниченного доступа.
3	**Охрана государственной тайны**	Государственная тайна (ГТ) как особый вид защищаемой информации; принципы и порядок отнесения сведений к ГТ; перечни сведений, составляющих ГТ. Степени секретности сведений и грифы секретности их носителей. Порядок рассекречивания сведений и их носителей. Распоряжение сведениями, составляющими ГТ. Ограничение прав собственности на информацию в связи с ее засекречиванием. Система защиты ГТ в РФ. Функции, задачи и полномочия органов защиты ГТ.
4	**Правовое регулирование распространения информации**	Разделение информации в зависимости от порядка ее предоставления или распространения. Общедоступная информация, распространение которой ограничено или запрещено и ее виды. Понятие организатора распространения информации в сети «Интернет» и его обязанности. Процедуры ограничения доступа к противозаконно распространяемой информации с использованием информационно-телекоммуникационных сетей. Обеспечение доступа к информации о деятельности государственных органов и органов местного самоуправления.
5	**Правовая охрана результатов интеллектуальной деятельности в сфере компьютерной информации**	Результаты интеллектуальной деятельности, которым предоставляется правовая охрана — интеллектуальная собственность. Виды интеллектуальных прав. Авторское право и его объекты в сфере компьютерной информации. Ответственность за нарушение авторского права. Правомерное использование программ для ЭВМ и баз данных.
6	**Лицензирование и сертификация в сфере ИБ**	Виды лицензируемой деятельности в области защиты информации. Порядок и системы лицензирования. Сертификация (подтверждение соответствия) средств защиты информации и защищенных автоматизированных систем. Системы и порядок сертификации ФСТЭК и ФСБ России.
7	**Преступления в сфере компьютерной информации**	Понятие об информационных и компьютерных преступлениях. Компьютер как орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Понятие компьютерной информации. Составы преступлений, предусмотренные ст. 272 – 274.1 УК РФ.
8	**Организация защиты информации (ЗИ). Компетенции специалистов в сфере ИБ**	Организационные основы ЗИ в учреждении, предприятии. Допуск персонала к защищаемой информации. Организация охраны и внутриобъектового режима. Организация выявления и расследования инцидентов ИБ. Взаимосвязь должностей, групп компетенций и видов профессиональной деятельности специалистов в области ИБ. Возможности сотрудничества с правоохранительными органами в сфере ИБ. Права и обязанности лица, выступающего в качестве специалиста или эксперта при расследовании административных правонарушений и уголовных дел.

9	**Правовое регулирование обработки персональных данных (ПДн). Обеспечение безопасности ПДн в организации**	Отношения, регулируемые ФЗ «О персональных данных». Понятия ПДн, оператора ПДн, информационной системы ПДн. Принципы и условия обработки ПДн. Обязанности и права оператора ПДн. Права субъекта ПДн. Биометрические ПДн и правила их обработки. Специальные категории ПДн и условия их обработки. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных». Меры, по обеспечению безопасности ПДн при их обработке. Понятие угроз безопасности ПДн. Определение уровня защищенности ПДн. Государственные органы, уполномоченные осуществлять контроль и надзор за выполнением мер по обеспечению безопасности ПДн. Ответственность за правонарушения (преступления) в сфере защиты ПДн. Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области ПДн.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения (учебный план № 6028, в. 3,)

Объем модуля (зач.ед.): 13
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Основные положения государственной политики в сфере обеспечения информационной безопасности (ИБ) РФ	**5**	**4**	4			**1**	**1**	1																					
2	Принципы правового регулирования отношений и основные понятия в сфере информации, информационных технологий и защиты информации. Ограничение доступа к информации	**19**	**14**	4	6	4	**5**	**5**	1	4																				
3	Охрана государственной тайны	**13**	**10**	4	3	3	**3**	**3**	1	2																				
4	Правовое регулирование распространения информации	**4**	**3**	4			**1**	**1**	1																					
5	Правовая охрана результатов интеллектуальной деятельности в сфере компьютерной информации	**4**	**3**	4			**1**	**1**	1																					
6	Лицензирование и сертификация в сфере ИБ	**22**	**16**	4	5	7	**6**	**6**	1	5																				
7	Преступления в сфере компьютерной информации	**12**	**4**	4			**8**	**1**	1				**7**	1																
8	Организация защиты информации (ЗИ). Компетенции специалистов в сфере ИБ	**14**	**4**	2			**10**	**1**	1				**9**	1																
9	Правовое регулирование обработки персональных данных (ПДн). Обеспечение безопасности ПДн в организации	**33**	**10**	4	3	3	**23**	**5**	7	3			**18**	2																
	Всего (час), без учета промежуточной аттестации:	**126**	**68**	**34**	**17**	**17**	**58**	**24**	**15**	**14**	**0**	**0**	**34**	**34**	**0**	**0**		**0**	**0**			**0**	**0**							
	Всего по дисциплине (час.):	**144**	**68**				**58**																				0	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

6.1. Лабораторные работы

7. ***Очная форма обучения***

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Разделение информации по категориям доступа. Присвоение меток документам.	4
3	2	Реализация мер по защите государственной тайны	3
6	3	Порядок лицензирования ФСТЭК. Порядок лицензирования ФСБ.	7
9	4	Письменное согласие работника на обработку персональных данных.	9
		Всего:	**17**

Ускоренная форма обучения (очно-заочная)
Не предусмотрено

7.1. Практические занятия

Очная форма обучения

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Инструкция пользователя. Ответственность за нарушение защиты информации ограниченного доступа.	6
3	2	Организация защиты государственной тайны.	3
6	3	Порядок лицензирования ФСТЭК. Порядок лицензирования ФСБ.	5
9	4	Письменное согласие работника на обработку персональных данных.	3
		Всего:	**17**

Ускоренная форма обучения (очно-заочная)

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Разделение информации по категориям доступа. Присвоение меток документам.	3
2	2	Инструкция пользователя. Ответственность за нарушение защиты информации ограниченного доступа.	3
3	3	Организация защиты государственной тайны. Реализация мер по защите ГТ.	4

6	4	Порядок лицензирования ФСТЭК.	3
6	5	Порядок лицензирования ФСБ.	2
9	6	Письменное согласие работника на обработку персональных данных.	3
		Всего:	**18**

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Исследование компьютерных журналов на наличие остаточной информации о преступной деятельности.*
- *Составление руководства по реагированию на инциденты информационной безопасности.*
- *Акт определения уровня защищенности персональных данных.*
- *Разработка модели угроз безопасности персональных данных при их обработке в информационных системах.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.4.1. Примерная тематика контрольных работ

Не предусмотрено

4.3.9. Примерная тематика коллоквиумов

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	**Активные методы обучения**						**Дистанционные образовательные технологии и электронное обучение**					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Основные положения государственной	*			*	*							

политики в сфере обеспечения информационной безопасности (ИБ) РФ												
2.Принципы правового регулирования отношений и основные понятия в сфере информации, информационных технологий и защиты информации. Ограничение доступа к информации	*			*								
3.Охрана государственной тайны		*			*							
4.Правовое регулирование распространения информации		*										
5.Правовая охрана результатов интеллектуальной деятельности в сфере компьютерной информации			*									
6.Лицензирование и сертификация в сфере ИБ			*		*							
7.Преступления в сфере компьютерной информации			*	*								
8.Организация защиты информации (ЗИ). Компетенции специалистов в сфере ИБ		*										
9.Правовое регулирование обработки персональных данных (ПДн). Обеспечение безопасности ПДн в организации	*				*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие для студентов вузов, обучающихся по специальностям 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М.В. Мецатунян .— 2-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2014 .— 256 с.

2. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям: 075200 - Компьютер. безопасность, 075500 - Комплекс. обеспечение информ. безопасности автоматизир. систем, 075600 - Информ. безопасность телекоммуникац. систем / [С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский, Е. Б. Белов, С. В. Полникова] ; под ред. С. Я. Казанцева .— М. : Академия, 2005 .— 240 с.

3. Загородников С.Н. Организационное и правовое обеспечение информационной безопасности. Ч. 1 / С. Н. Загородников, А. А. Шмелев .— М. : Новые технологии : Информационные технологии, 2005 .— 32 с.

4. Загородников С.Н. Организационное и правовое обеспечение информационной безопасности. Ч. 2 / С. Н. Загородников, А. А. Шмелев .— М. : Новые технологии : Информационные технологии, 2006 .— 32 с.

9.1.2.Дополнительная литература

1. Рассолов, И. М. Интернет-право / И.М. Рассолов .— Москва : Юнити-Дана, 2015 .— 143 с.

2. Копылов, Виктор Александрович. Информационное право : учебник / В. А. Копылов ; М-во образования РФ, Моск. гос. юрид. акад. — Изд. 2-е, перераб. и доп. — М. : Юристъ, 2005 .— 511 с.

3. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия : учеб. пособие / Г. А. Остапенко, Е. А. Мешкова ; под ред. В. Г. Кулакова .— Москва : Горячая линия - Телеком, 2008 .— 208 с.

4. Макнамара, Дж. Секреты компьютерного шпионажа. Тактика и контрмеры / Д. Макнамара ; пер. с англ. А. В. Бутко ; под ред. С. М. Молявко .— М. : БИНОМ. Лаборатория знаний, 2008 .— 536 с.

5. Галатенко, В. А. Стандарты информационной безопасности. Курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. технологий / В. А. Галатенко ; под ред. В. Б. Бетелина .— 2-е изд. — Москва : Интернет-Университет Информационных Технологий, 2009 .— 264 с.

9.2.Методические разработки

1. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Т. 1. Законодательные акты РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ / Урал. гос. техн. ун-т - УПИ, Регион. учеб.-науч. центр по проблемам информ. безопасности ; [авт.-сост. Н. А. Гайдамакин] .— Екатеринбург : Гриф, 2006 .— 658 с. ; 29 см .— Библиогр. в тексте, библиогр. в примеч. — ISBN 5-98058-021-2.

2. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Т. 2. Ведомственные нормативные правовые акты и руководящие документы / Урал. гос. техн. ун-т - УПИ, Регион. учеб.-науч. центр по проблемам информ. безопасности ; [авт.-сост. Н. А. Гайдамакин] .— Екатеринбург : Гриф, 2006 .— 740 с.

9.3.Программное обеспечение

MS Office

9.4. 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

9.5.Электронные образовательные ресурсы

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

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.
6.2.Процедуры текущей и промежуточной аттестации по дисциплине
Очная форма обучения

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,8		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*8,1-7*	*25*
Домашняя работа №2	*8,8-15*	*25*
Домашняя работа №3	*8,8-15*	*25*
Домашняя работа №4	*8,8-15*	*25*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,2		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение практический заданий	*8,1-15*	*100*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Отчет по лабораторным работам	*8,8-15*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

Ускоренная форма обучения (очно-заочная)

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,8**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*8,1-7*	*25*
Домашняя работа №2	*8,8-15*	*25*
Домашняя работа №3	*8,8-15*	*25*
Домашняя работа №4	*8,8-15*	*25*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,2		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение практический заданий	*8,1-15*	*100*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено
6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

−в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;

−при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий *Не предусмотрено*

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Источники угроз информационной безопасности.
2. Виды информации ограниченного доступа. Основные условия режима ограниченного доступа к информации.
3. Служебная тайна. Отнесение информации к служебной тайне.
4. Ответственность за правонарушения в сфере коммерческой тайны.
5. Порядок установления и изменения грифа ограничения документов и изделий.
6. Порядок оформления допуска к сведениям, имеющим гриф ограничения.
7. Государственная тайна. Объект и субъекты правоотношений в области государственной тайны.
8. Государственная тайна. Принципы отнесения сведений к государственной тайне.
9. Функции, задачи и полномочия органов защиты государственной тайны.
10. Понятие о техническом регулировании в области защиты информации.
11. Обеспечение правовой охраны конфиденциальной информации.
12. Общедоступная информация. Виды общедоступной информации.
13. Ограничение доступа к противозаконно распространяемой информации с использованием информационно-телекоммуникационных сетей.
14. Виды интеллектуальных прав. Авторское право и его объекты в сфере компьютерной информации.
15. Виды ответственности за нарушение авторского права.
16. Порядок и лицензирования и сертификации.
17. Сертификация средств защиты информации. Реестры сертифицированных средств.
18. Компьютерная информация.
19. Реализация преступлений с использованием компьютера.
20. Взаимосвязь должностей, групп компетенций и видов профессиональной деятельности специалистов в области ИБ.
21. Сотрудничество с правоохранительными органами.
22. Требования по защите персональных данных.
23. Общедоступные источники персональных данных.
24. Специальная категория персональных данных. Письменное согласие на обработку.

25. Обязанности оператора при обработке персональных данных.
26. Меры по обеспечению безопасности персональных данных при их обработке. П
27. Порядок уведомления оператором уполномоченного органа по защите прав субъектов персональных данных.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль ***Информационная безопасность***	**Код модуля** № 1140576/33630 УП 6938
Образовательная программа ***Информационная безопасность информационно-аналитических систем***	**Код ОП** ***10.05.04/01.01***
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки ***Информационная безопасность информационно-аналитических систем***	**Код направления и уровня подготовки** ***10.05.04***
Уровень подготовки ***специалист***	
ФГОС ВО ***Информационная безопасность информационно-аналитических систем***	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: № 1514 1 декабря 2016 г.

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Лучинин Александр Сергеевич	К.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам. председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению видов, источников и носителей защищаемой информации. В дисциплине рассматриваются демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники; структура, классификация и основные характеристики технических каналов утечки информации. Изучаются возможности видов технической разведки; концепция и методы инженерно-технической защиты информации. А также излагаются методы расчета и инструментального контроля показателей защиты информации.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способностью анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности (ОПК-1);
- способностью применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7).
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);
- способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10);
- способность разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности (ПК-11);
- способность разрабатывать программное и иные виды обеспечения специальных ИАС (ПК-12);
- способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-13).
- способность использовать специальные ИАС для решения задач в сфере профессиональной деятельности (ПК-14);
- способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях (ПК-15).

В результате освоения дисциплины студент должен:

Знать:

- сущность и понятия информации, информационной безопасности и характеристику ее составляющих;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- технические каналы утечки информации;
- возможности технических средств перехвата информации;
- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- организацию защиты информации от утечки по техническим каналам на объектах

информатизации;
- принципы работы элементов и функциональных узлов электронной аппаратуры;
- уязвимости основных телекоммуникационных технологий;
- технологии, средства и методы обеспечения информационной безопасности телекоммуникационных систем.

Уметь:
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- анализировать и оценивать угрозы информационной безопасности объекта;
- осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;
- измерять и рассчитывать основные характеристики сигналов и помех;
- пользоваться метрологическим обеспечением экспериментального исследования телекоммуникационных систем и обеспечения информационной безопасности;
- анализировать безопасность функционирования телекоммуникационных систем.

Владеть (демонстрировать навыки и опыт деятельности):
- профессиональной терминологией в области информационной безопасности;
- методами и средствами технической защиты информации;
- методами расчета и инструментального контроля показателей технической защищенности информации;
- навыками безопасного использования технических средств в профессиональной деятельности;
- навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений;
- навыками рационального выбора средств и методов защиты информации объектов информатизации;
- навыками использования современной измерительной аппаратуры при проведении измерений в телекоммуникационных системах;
- навыками анализа безопасности функционирования телекоммуникационных систем.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*7*
1.	**Аудиторные занятия**	51	51	51
2.	Лекции	34	34	34
3.	Практические занятия	0	0	0
4.	Лабораторные работы	17	17	17
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	93	10.65	93
6.	**Промежуточная аттестация**	К, Э	2.33	К, Э
7.	**Общий объем по учебному плану, час.**	144	63,98	144
8.	**Общий объем по учебному плану, з.е.**	4		4

Заочная форма обучения не предусмотрена

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

		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. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 14
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязычной литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Концепция технической защиты информации	**10**	**8**	8			2	2	2																						
2	Теоретические основы технической защиты информации	**50**	**20**	8		12	30	12	2		10		18						1												
3	Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации	**30**	**14**	9		5	16	8	3		5													8	1					
4	Организационные основы технической защиты информации	**36**	**9**	9			27	3	3				24									1								
	Всего (час), без учета промежуточной аттестации:	**126**	**51**	**34**		**17**	75	25	10		15		42						18			24		**8**	**8**					
	Всего по дисциплине (час.):	**144**	**51**				**75**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
2	1	Обнаружение каналов утечки информации, обусловленных ПЭМИ. Оценка количественных характеристик и степени опасности	2
2	2	Исследование возможностей и характеристик средств защиты от утечки (перехвата) информации по каналам ПЭМИ	2
2	3	Исследование эффективности применения средств защиты от перехвата информации по каналам ПЭМИ. Проведение аттестационных исследований	2
2	4	Исследование каналов утечки информации, образованных проводными коммуникациями	2
2	5	Исследование возможностей и характеристик средств защиты от утечки (перехвата) информации в проводных линиях	2
2	6	Исследование эффективности применения средств защиты от перехвата информации в проводных линиях. Проведение аттестационных исследований	2
3	7	Исследование методов обнаружения закладных устройств, излучающих в радиочастотном диапазоне.	1
3	8	Исследование возможностей и методов борьбы со средствами разведки, использующими радиоканал для передачи информации	2
3	9	Исследование методов и аппаратуры защиты телефонной проводной линии от негласного прослушивания с помощью средств разведки	2
		Всего:	**17**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

Не предусмотрено

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

- *Обзор методов и формулирование требований к комплексу контроля защищенности проводной линии от перехвата информации с помощью средств разведки. Количественные характеристики проводной линии и требования по защищенности формулируются индивидуально для каждого студента.*
- *Обзор методов и формулирование требований к комплексу контроля защищенности средств вычислительной техники от перехвата информации с помощью средств разведки по каналам ПЭМИН. Количественные характеристики защищаемых систем вычислительной техники и требования по защищенности формулируются индивидуально для каждого студента.*
- *Обзор методов и формулирование требований к комплексу контроля защищенности информации от перехвата с помощью специальных средств разведки, передающих информацию по радиоканалу. Количественные характеристики средств разведки и требования по защищенности формулируются индивидуально для каждого студента.*

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Задания на курсовые работы формулируются индивидуально каждому студенту.

Ниже приведены примеры нескольких заданий:

Задание №1.

В помещении, расположенном на первом этаже и имеющем размеры 6×5×2,6 м работает компьютер, создающий побочные электромагнитные излучения в диапазоне частот от 300 до 1000 МГц, излучающиеся случайными антеннами и имеющие напряженность электрического поля на расстоянии 2 м от источника 50 мкВ/м во всем диапазоне. Измерение напряженности поля проведено узкополосным приемником с полосой пропускания 100 кГц.

Для обеспечения защищенности компьютера от утечки информации в соответствии с нормами требуется отношение мощностей сигнала и шума: $P_C/P_Ш = 0,1$ (-10 дБ) в полосе частот, занимаемой информационным сигналом. Шум - это тепловой шум антенны.

♦ Определите существующее отношение сигнал/шум на границах помещения (при условии, что компьютер расположен в центре помещения, и доступ снизу исключен). Принять, что на всех частотах прием сигналов ведется приемником с антенной типа симметричного полуволнового вибратора (настраиваемого на каждой частоте). Сопротивление излучения антенны равно 73 Ом. Полосы пропускания приемника принять соответствующими сигналам видеосистемы компьютеров (для современных компьютеров 50 МГц) и излучению клавиатуры (примерно 100 кГц).

♦ Определите радиусы зоны II (R2) для обеих полос сигналов, исходя из заданного отношения сигнал/шум $P_C/P_Ш = 0,1$.

♦ Определите во сколько раз необходимо увеличить спектральную плотность шумов для уменьшения радиуса R2 до границ помещения.

♦ Какова должна быть мощность широкополосного генератора, имеющего ширину спектра излучения от 10 до 1000 МГц, для обеспечения нужного уровня спектральной плотности шума, при условии, что генерируется шум с равномерной спектральной плотностью и со спектральной плотностью изменяющейся по закону: $S(\omega) = S_0/\omega^4$ (реальный генератора шума, например, ГШ 1000). Предполагается, что генератор шума будет располагаться рядом с компьютером.

Задание №2.

Для защиты переговоров по телефону от подслушивания при помощи диктофонов и других устройств, которые могут быть подключены к телефонному кабелю, в

телефонную линию подается высокочастотный шум. Интенсивность шума должна быть достаточно высокой, чтобы эффективно противодействовать подслушивающим устройствам. Спектр шума не должен перекрываться со спектром речевого сигнала (в телефонных системах речевой сигнал занимает область частот от 300 Гц до 3,4 кГц). В то же время он должен максимально приближаться к спектру речевого сигнала, чтобы его нельзя было отфильтровать простым фильтром в подслушивающем устройстве.

Для нормальной работы телефонной системы телефонные аппараты и другие элементы преобразования речевого сигнала (устройства на городской АТС или локальной мини АТС) должны быть снабжены фильтрами нижних частот с характеристиками, обеспечивающими разделение шума и речевого сигнала.

Требуется выбрать тип и рассчитать фильтр нижних для выделения речевого сигнала из смеси с шумом при следующих характеристиках речевого сигнала и шума.

♦ Речевой сигнал имеет действующее значение напряжения 1 В.

♦ Спектр речевого сигнала ограничен частотами 300 Гц – 3,4 кГц и имеет в этом диапазоне закон изменения спектральной плотности мощности $W(\omega) \sim 1/\omega$.

♦ Маскирующий шум имеет действующее значение напряжения 10 В.

♦ Спектр шума занимает область частот от 5 кГц до 50 кГц и имеет постоянную спектральную плотность мощности в этом диапазоне.

♦ При выделении речевого сигнала необходимо обеспечить превышение действующего значения сигнала над шумом более 20 дБ.

♦ При проектировании и расчете фильтра считать, что линия нагружена на стандартное сопротивление 600 Ом.

♦ Неравномерность частотной характеристики фильтра в полосе пропускания не должна превышать 3 дБ.

Определить характерные частоты и порядок фильтра. Выбрать и обосновать вид реализации фильтра (пассивный, активный или другой). Выполнить расчет элементов фильтра. Выбрать радиокомпоненты для реализации фильтра. Оценить габаритные размеры фильтра. Оценить возможность использования подобного фильтра в малогабаритном закладном устройстве.

Задание №3.

Рассчитайте быстродействие работы сканирующего приемника под управлением компьютера по программе (например, «Филин»). Приемник управляется компьютером через интерфейс RS232 с максимальной скоростью передачи данных 115 Кбит/с. В процессе одного шага сканирования достаточно в прямом (от компьютера приемнику) и в обратном направлении передавать по 8 байт (команда перехода на следующую частоту и уровень сигнала, измеренный на данной частоте).

♦ Определите время необходимое для обзора диапазона частот от 1 МГц до 2000 МГц с шагом 10 кГц определяемое быстродействием интерфейса. Учтите, если необходимо, время, требуемое для выработки команды и записи данных компьютером.

♦ Рассчитайте длительность обзора указанного диапазона частот с данным шагом определяемое переходными процессами в полосовом фильтре приемника.

Фильтр должен иметь полосу пропускания 10 кГц, ослабление при расстройке на 10 кГц от центральной частоты должно составлять 60 дБ.

Время переходного процесса должно обеспечивать динамический диапазон по амплитуде наблюдаемых сигналов не менее 60 дБ.

Выбрать и рассчитать полосовой фильтр, рассчитать его переходную характеристику, по которой и определить длительность переходного процесса.

♦ Рассчитайте длительность обзора указанного диапазона частот с данным шагом, определяемую временем перестройки частоты синтезатора частот. Длительность перехода на следующую частоту составляет от 10/ΔfC до 100/ΔfC, где ΔfC – шаг перестройки синтезатора частот.

♦ Определите суммарную длительность обзора заданного диапазона частот, обусловленную всеми названными факторами. Укажите, какие еще причины могут замедлять скорость сканирования приемника.

♦ Предложите метод ускоренного обзора широкого диапазона частот каким-либо устройством.

4.3.8. Примерная тематика контрольных работ

– *Методы обнаружения закладных устройств, излучающих в радиочастотном диапазоне.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Концепция технической защиты информации					*							
2.Теоретические основы технической защиты информации				*								
3.Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации				*	*							
4.Организационные основы технической защиты информации					*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

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.

9.1.2.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.

9.2.Методические разработки

1. Исследование технических каналов утечки информации и методов борьбы с ними : метод. указания к лаб. работам по дисциплине "Техн. средства и методы защиты информации" для студентов специальности 075600 - Информ. безопасность телекоммуникац. систем / Урал. гос. техн. ун-т - УПИ ; [сост. А. С. Лучинин ; науч. ред. А. П. Мальцев] .— Екатеринбург : УГТУ-УПИ, 2004 .— 39 с.

9.3.Программное обеспечение

Word, Excel

9.4. Базы данных, информационно-справочные и поисковые системы

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

9.5.Электронные образовательные ресурсы

Не предусмотрено

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Занятия проводятся в лаборатории технических средств защиты информации (Р-325, Р-413), оснащенной следующим специализированным оборудованием:

1. Селективный микровольтметр SMV-8.5;
2. Селективный нановольтметр UNIPAN 233;
3. Сканирующий приемник AR 3000A;
4. Сканирующий приемник ICOM PCR 1000;
5. Компьютер IBM Pentium, упрвляющая программа "Филин";
6. Многофункциональный поисковый прибор SR031P;
7. Генератор шума "Гром-ЗИ4";
8. Контроллер телефонных линий КТЛ 400;
9. Генератор Г3-112;
10. Установка для исследования утечки информации с монитора ПК;
11. Макеты радиомикрофонов;
12. Макет сетевого фильтра;
13. Ультразвуковой излучатель для исследования методов борьбы с радиомикрофонами;
14. Миниатюрные видеокамеры (2 экз.);
15. Кассетный диктофон Olimpus L400;
16. Цифровой диктофон Edik mini;
17. Макеты проводных линий;
18. Макеты излучающих печатных плат;
19. Анализатор спектра E4402B (Agilent);
20. Измерительный приемник ESPI 3 (Rohde&Scwarz);
21. Высокочастотный генератор N5181A (100 кГц – 3 ГГц) (Agilent);
22. Низкочастотный генератор AM300 (R&S);
23. Низкочастотный генератор SFG 2010;
24. Осциллограф GDS – 806S (до 60 МГц);
25. Осциллограф С-103 (двух лучевой, четырех канальный);
26. Имитатор закладных устройств многофункциональный ИМФ-2 (4 штуки);
27. Индикатор напряженности поля ST007;
28. Сканирующий поисковый прибор PROTEC;
29. Комплекс контроля ПЭМИ «Сигурд»;
30. Настольный ПК с ЖКИ монитором и устройством ввода аналоговых данных
31. Сканирующий приемник – постановщик прицельной помехи «Скорпион»
32. Обнаружитель скрытых видеокамер «Алмаз»;
33. Подавитель диктофонов, сотовых телефонов GSM, ПЭМИ «Багет 6»
34. Адаптер Wi-Fi (2 штуки);
35. Адаптер Wi-Max (2 штуки).

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Расчетно-графическая работа	*7,1-7*	*60*
Контрольная работа	*7,8-15*	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,4		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение лабораторных работ № 1-9	*7,8-15*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

4. Курсовая работа: коэффициент значимости совокупных результатов курсовой работы – 1.0		
Текущая аттестация курсовой работы	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям – 1,0		
Промежуточная аттестация по практическим/семинарским занятиям– нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям – 1,0**		

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с наличием Дисциплины и ее аналогов, по которым возможно тестирование, на портале СМУДС УрФУ, возможно тестирование в рамках НТК.

ПРИЛОЖЕНИЕ 3

к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.
2. Методы и средства защиты информации в системах с проводными линиями. Типы проводных линий. Виды угроз, создаваемых проводными линиями. Оценка степени паразитных связей в линиях и уровней паразитных излучений, создаваемых проводными линиями.
3. Паразитные каналы утечки информации в телефонных системах и телефонных кабелях. Акустоэлектрические преобразования в телефонных аппаратах при опущенной трубке. Оценка уровней сигналов и уровней помех в телефонных линиях. Оценка реальности образования канала утечки. Защита от утечки с использованием диодных устройств типа «Гранит», «Корунд» и других. Особенности работы этих устройств в современных электронных аппаратах.
4. Применение генераторов шума для закрытия канала утечки за счет акустоэлектрического преобразования. Виды зашумления телефонных линий с целью закрытия каналов утечки информации.
5. Высокочастотное навязывание в телефонных системах. Механизмы взаимодействия акустического сигнала с высокочастотным сигналом навязывания. Оценка реальности канала утечки за счет высокочастотного навязывания. Оценка чувствительности метода.
6. Преднамеренно созданные каналы утечки по проводным линиям. Включение закладных устройств с передачей информации по проводам. Маскировка сигналов путем использования занятых проводных линий: радиотрансляционных сетей, телефонных линий, сетей электропитания и других. Возможности и методы

выделения сигналов в проводных линиях от помех. Компенсация помех. Адаптивные автокомпенсаторы.

7. Аппаратура выделения информации методом ВЧ навязывания, возможности и методы обеспечения высокой чувствительности. Меры борьбы с ВЧ навязыванием. Аппаратура контроля за утечкой информацией по каналам ВЧ навязывания.
8. Закладные устройства в системах с проводными коммуникациями. Устройства съема речевой информации в телефонных линиях. Методы подключения устройств. Использование диктофонов. Методы защиты от описанных закладных устройств. Аппаратура контроля и защиты от утечки информации по проводным линиям. Недостатки существующей аппаратуры.
9. Электрические характеристики и принцип работы городских телефонных линий. Возможные способы подключения закладных устройств к телефонным линиям. Количественные характеристики возмущений, вносимых закладными устройствами, и оценка возможности обнаружения закладных устройств. Примеры построения телефонных радио ретрансляторов (закладных устройств) с питанием от телефонных линий и оценка степени их влияния на параметры телефонных линий.
10. Методы защиты телефонных (и других проводных) линий от утечки информации через закладные устройства, параллельные телефоны и другими путями:
11. Способы реализации данных методов. Достоинства и недостатки. Проблемы реализации.
12. Применение фильтров для борьбы с утечкой информации по проводным линиям. Требования к характеристикам фильтров. Фильтры, предназначенные для защиты от утечки информации по сети 220 В. Особенность сетевых фильтров. Проектирование сетевых фильтров. Схемная реализация фильтров: независимые фазные фильтры; связанные фильтры. Реализация индуктивных и емкостных элементов сетевых фильтров. Ограничения, накладываемые на характеристики фильтров эксплуатационными требованиями.
13. Включение фильтров. Синфазные и противофазные сигналы и наводки в фильтрах. Заземление фильтров. Фильтры, предназначенные для защиты от мощных импульсных помех и преднамеренных воздействий. Меры защиты других проводных линий: провода пожарной и охранной сигнализаций, провода линий оповещения, городская трансляционная сеть, кабели компьютерных сетей, другие проводные линии.
14. Каналы утечки информации образованные электромагнитным излучением. Утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Виды каналов утечки за счет ПЭМИН. Основные средства (обработки конфиденциальной информации). Образование каналов утечки за счет наводок с основных средств на вспомогательные. Определение количественных характеристик цепей паразитных связей. Паразитные емкостная, индуктивная и связи.
15. Закладные устройства, использующие радиоканал. Средства индивидуальной радиосвязи: сотовые телефоны, бесшнуровые телефонные аппараты, пейджеры и другие.
16. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Возможности современной радиоэлектроники по построению закладных устройств.
17. Проблемы обнаружения и борьбы с закладными устройствами (ЗУ). Обеспечение энергетической скрытности (ЗУ). Потенциал радиоканала. Оценка эффективности антенн передатчиков и радиоприемников. Оценка минимальной мощности передатчиков (ЗУ). Оценка пороговой чувствительности радиоприемников.
18. Приборы для обнаружения электромагнитных излучений. Широкополосные индикаторы напряженности поля. Узкополосные сканирующие приемники.

Проблемы, связанные с их применением. Принцип построения названных приборов. Проблемы построения сканирующих приемников. Обеспечение высокой избирательности по паразитным каналам приема. Обеспечение высокой скорости обзора широкого частотного диапазона.

19. Методы обнаружения закладных устройств и паразитных излучений с применением широкополосных индикаторов и сканирующих приемников. Мониторинг эфира. Акустическая завязка. Акустическая локация. Корреляционная обработка принятых сигналов. Проблемы, возникающие при обнаружении закладных устройств.
20. Закладные устройства, использующие сложные сигналы. Возможности реализации таких устройств на современной элементной базе. Возможности обнаружения таких устройств. Направление построения аппаратуры для обнаружения излучений со сложными сигналами.
21. Построение радиоканалов передачи данных (сообщений) с цифровой обработкой сигналов и с использованием сложных широкополосных несущих. Возможности и примеры построения радиопередатчиков со сложными сигналами. Микросхемы XE1202, AD9850. Построение радиоприемников сложных сигналов: с псевдослучайной перестройкой частоты. Проблемы синхронизации.
22. 20. Возможности и примеры построения радиоприемников приема сложных сигналов с фазовой манипуляцией. Построение устройств обработки сигналов на регистрах сдвига (цифровые корреляторы и согласованные фильтры). Использование ПАВ устройств (согласованные фильтры и конвольверы). Проблемы синхронизации.
23. Методы защиты от утечки информации через закладные устройства, использующие радиоканал, и ПЭМИ. Экранирование. Эффективность экранирования высокочастотного электромагнитного излучения сплошным металлическим экраном. Влияние щелей и отверстий. Эффективность экранирования сетчатым экраном.
24. Активные методы защиты. Эффективность зашумления широкополосным шумовым излучением. Эффективность зашумления ультразвуком.
25. Организованные каналы утечки (съема) информации – закладные устройства. Закладные устройства с проводными каналами передачи. Использование проводов сети 220 В и других проводных линий. Закладные устройства с радиоканалом. Диапазоны частот, мощность передатчиков, виды модуляции, виды сигналов, используемые в закладных устройствах.
26. Определение количественных характеристик цепей паразитных связей. Паразитные емкостная, индуктивная связи. Определение уровней наводок через паразитную емкость между приборами и проводниками. Определение уровней наводок за счет контуров с током (взаимной индуктивности). Излучение случайных антенн – электрических и магнитных диполей.
27. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Магнитные экраны на низких частотах. Магнитные экраны на высокой частоте. Поверхностный эффект и токи Фуко. Соотношения и количественные показатели степени экранирования электростатических и магнитных экранов.
28. Борьба с утечкой информации по техническим каналам. Методы обнаружения утечки информации за счет побочных излучений и излучений закладных устройств. Широкополосные индикаторы напряженности поля. Проблемы их применения. Сканирующие узкополосные приемники. Требования к характеристикам. Тактика применения. Проблемы использования.
29. Защита информации от утечки в телефонных каналах связи. Каналы утечки информации: прямой перехват переговоров путем подключения к телефонной линии; утечка информации по линии при положенной трубке за счет микрофонного

эффекта и других акустоэлектрических преобразований; перехват информации при помощи закладных устройств (типы и способы подключения); перехват информации за счет высокочастотного навязывания. Методы борьбы с утечкой информации. Зашумление телефонной линии. Виды и способы зашумления.

30. Побочные электромагнитные излучения радиоэлектронных средств. Излучения гетеродинов радиоприемников. Излучения элементов компьютеров. Методика и аппаратура контроля уровня побочных излучений. Методика определения информативности побочных излучений.
31. Основные методы защиты информации техническими средствами. Охрана источников информации. Скрытие достоверной информации. Дезинформирование.
32. Методы локализации и обнаружения закладных устройств. Акустическое зондирование и определение дальности до закладного устройства. Корреляционная обработки акустических сигналов для локализации закладных устройств. Анализ уровня высших гармоник в излучении закладных устройств.
33. Нелинейные локаторы. Принцип действия. Проблемы применения.
34. Методика и аппаратура для измерения уровней наведенных сигналов из одних проводных линий в другие. Оценка (измерение) наведенных напряжений и токов в проводных линиях от электронных приборов (основных средств обработки конфиденциальной информации).
35. Методика и аппаратура наблюдения за радио излучениями в эфире с целью выявления каналов утечки информации за счет ПЭМИН и закладных устройств (мониторинг эфира). Требования к аппаратуре наблюдения. Обоснование возможности выявления каналов утечки информации. Характеристика возможностей поисковой программы «Филин».
36. Методика и аппаратура для измерения характеристик канала передачи сигналов по проводам сети 220 В. Проблемы, возникающие при использовании данного канала для передачи данных.
37. Методика измерения характеристик излучения проводных линий при помощи прибора ST 031P «Пирания». Приборы, необходимые для измерений. Сравнительные характеристики излучения проводных линий различных конструкций.
38. Методика измерения уровней излучения приборов и элементов приборов (например, печатных плат). Аппаратура, необходимая для проведения этих измерений.
39. Методика обнаружения и измерения уровней информативных паразитных излучений компьютеров. Методика оценки радиуса R2 (минимального расстояния до компьютера, на котором отношение сигнал/шум не превышает заданной величины). Аппаратура, с помощью которой можно сделать такие измерения.
40. Методика оценки эффективности зашумления паразитных излучений компьютера и зашумления излучения закладного устройства с радиоканалом. Аппаратура, необходимая для проведения измерений.
41. Методика определения мощности излучения закладных устройств и других источников. Экспериментальное определение дальности обнаружения излучения закладного устройства.
42. Поиск, локализация и обнаружение закладных устройств при помощи широкополосного индикатора напряженности поля «Пирания». Причины, ограничивающие возможности данного прибора. Пути его совершенствования.
43. Методика и аппаратура для наблюдения и измерения характеристик канала утечки информации за счет акусто-электрического преобразования в электронной аппаратуре. Измерение паразитной частотной модуляции, возникающей в генераторе сигналов.

44. Методика и аппаратура для оценки эффективности зашумления закладного устройства, включенного в телефонную линию, при использовании прибора КТЛ 400.
45. Характеристика методов обнаружения закладных устройств, включенных в телефонную линию, реализованных в приборе КТЛ 400 и других методов. Характеристика проблем, возникающих при решении данной задачи.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	Учетные данные
Модуль ***Информационная безопасность***	**Код модуля** № 1140576/33630 УП 6938
Образовательная программа ***Информационная безопасность информационно-аналитических систем***	**Код ОП** ***10.05.04/01.01***
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки ***Информационная безопасность информационно-аналитических систем***	**Код направления и уровня подготовки** ***10.05.04***
Уровень подготовки ***специалист***	
ФГОС ВО ***Информационная безопасность информационно-аналитических систем***	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: № 1514 1 декабря 2016 г.

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Сафиуллин Н.Т	К.т.н.,	доцент	Департамент Информационных технологий и автоматики	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам.председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ПРОГРАМНОНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

1.1.Аннотация содержания дисциплины

Дисциплина «Программно-аппаратные средства защиты информации» относится к модулю по «Информационная безопасность». Дисциплина «Программно-аппаратные средства защиты информации» знакомит с архитектурой современных вычислительных машин, программированием на аппаратном уровне, возможностями и особенностями применяемых аппаратных решений на примере IBM-совместимых персональных компьютеров. Предполагается что изучающие настоящую дисциплину прослушали курсы «Архитектура ЭВМ» и «Ассемблер» и владеют приемами программирования на языке ассемблера для процессоров Intel x86.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

– способностью анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности (ОПК-1);

– способностью применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7).

– способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);

– способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10);

– способность разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности (ПК-11);

– способность разрабатывать программное и иные виды обеспечения специальных ИАС (ПК-12);

В результате освоения дисциплины студент должен:

Знать:

- базовую архитектуру, шины и интерфейсы современных вычислительных машин;
- аппаратную организацию компьютеров;
- принципы обмена данными с внешними устройствами на уровне ОС, BIOS и портов ввода-вывода.

Уметь:

- программировать на аппаратном уровне, перехватывать и обрабатывать прерывания;
- оптимально выбирать алгоритмы и структуры данных для решения поставленных задач;
- записывать алгоритмы на языке ассемблера, тестировать и отлаживать полученные программы.

Владеть:

- техникой синхронного и асинхронного программирования;
- техникой программирования устройств ввода-вывода, включая обработку прерываний..

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	6
1.	**Аудиторные занятия**	**68**	**68**	**68**
2.	Лекции	34	34	34
3.	Практические занятия	34	34	34
4.	Лабораторные работы	0	0	0
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**22**	**10,2**	**22**
6.	**Промежуточная аттестация**	18	**2,33**	**18(э)**
7.	**Общий объем по учебному плану, час.**	144	80,53	144
8.	**Общий объем по учебному плану, з.е.**	4		4

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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 арифметико-логическое 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. BUS-mastering. 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.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Объем модуля (зач.ед.): 6
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	Всего по разделу, теме (час.)	Всего аудиторной работы (час.)	Лекции	Практические занятия	Лабораторные работы	Всего самостоятельной работы студентов (час.)	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	Всего (час.)	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	Всего (час.)	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
PI	Принципы Фон-Неймана и общее устройство современного компьютера.	7,2	6	6			1,2	1,2	1,2	0			0											0						
PII	Работа с внешними устройствами	2,4	2	2			0,4	0,4	0,4	0			0											0						
PIII	Механизм прерываний	21,6	18	4	14		3,6	3,6	0,8	2,8			0											0						
PIV	Контроллер прерываний	9,2	6	4	2		3,2	1,2	0,8	0,4			2	1										0						
PV	Организация ввода-вывода	23,8	18	4	14		5,8	3,8	0,8	3			2	1										0						
PVI	Таймеры, измерение времени и генерация звука	9,2	6	4	2		3,2	1,2	0,8	0,4			2	1										0						
PVII	Компьютерная память	2,4	2	2			0,4	0,4	0,4	0			0											0						
PVIII	Прямой доступ к памяти	2,4	2	2			0,4	0,4	0,4	0			0											0						
PIX	Системные шины. ISA, EISA, PCI	11,8	8	6	2		3,8	1,8	1,4	0,4			2	1										0						
	Всего (час), без учета промежуточной аттестации:	**126**	**68**	**34**	**34**	**0**	**22**	**14**	**7**	**7**	**0**	**0**	**8**					**0**		7				**0**		**0**				

	Всего по дисциплине (час.):	**144**	**68**		**58**	В т.ч. промежуточная аттестация	**0**	**18**	**0**	**0**

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

не предусмотрено

4.2. Практические занятия

Код раздела, темы	Номер занятия	Тема занятия	Время на проведение занятия (час.)
PIII	1	Создание резидентных программ	6
PIII	2	Перехват векторов прерываний	8
PIV	6	Программирование движущихся объектов	2
PV	3	Вывод на экран	6
PV	4	Ввод данных с клавиатуры	8
PVI	5	Генерация звука	2
PIX	7	Работа с шиной PCI	2
		Всего:	34

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- Перехват векторов прерываний
- Программирование движущихся объектов
- Вывод на экран; ввод данных с клавиатуры
- Работа с шиной PCI

4.3.2. Примерный перечень тем графических работ

не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

не предусмотрено

4.3.8. Примерная тематика контрольных работ

не предусмотрено

4.3.9. Примерная тематика коллоквиумов

не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисци-	Активные методы обучения	Дистанционные образователь-ные технологии и электронное

плины							обучение						
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
PI- PIX				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. М. Гук, Аппаратные интерфейсы ПК Энциклопедия. СПб, «Питер», 2002. http://libarch.nmu.org.ua/handle/GenofondUA/4726
2. 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
3. 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
4. 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-vol-2a.pdf
5. 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-vol-2b.pdf
6. 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
7. 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
8. 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-sdm-vol-3a.pdf

9. 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-sdm-vol-3b.pdf
10. 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-sdm-vol-3c.pdf
11. 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-sdm-vol-3d.pdf
12. Ю.С.Лукач, Базовая система ввода-вывода, Свердловск, Инженерно-техническое бюро, 1990 Книга выдается в электронном виде с согласия автора.
13. 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.

9.1.2.Дополнительная литература

1. 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
2. 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
3. Intel® 64 and IA-32 architectures optimization reference manual https://software.intel.com/sites/default/files/managed/9e/bc/64-ia-32-architectures-optimization-manual.pdf
4. Intel® architecture instruction set extensions programming reference https://software.intel.com/sites/default/files/managed/c5/15/architecture-instruction-set-extensions-programming-reference.pdf
5. 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
6. 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-core-processor-uncore.pdf
7. Intel® Virtualization Technology for Directed I/O architecture specification https://software.intel.com/sites/default/files/managed/c5/15/vt-directed-io-spec.pdf

9.2.Методические разработки

не используются

9.3.Программное обеспечение

MS DOS v 3.15 и выше с набором системных утилит.
ОС Ubuntu 14.04 и выше с набором системных утилит

9.4. 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

9.5.Электронные образовательные ресурсы

не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

1. Лекционная аудитория, оснащенная компьютером и видеопроектором.
2. Класс IBM совместимых ПЭВМ.

.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины – 0,5.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – k лек. = 0,1		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	8, 1-17	100
Весовой коэффициент значимости результатов текущей аттестации по лекциям – k тек.лек.=0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – k пром.лек.=0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – k прак. =0,9		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение практических /семинарских занятий	8,1-17	0
Выполнение работы на занятии	8,1-17	40
СРС - выполнение домашних работ	8,1-17	60
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– k тек.прак.=1		
Промежуточная аттестация по практическим/семинарским занятиям– *не предусмотрен* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– k пром.прак. =0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – k лаб. =0		
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям– 0		
Промежуточная аттестация по лабораторным занятиям– **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 6	**1**

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

– НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения домашних работ в рамках учебных занятий

Используя вызовы обработчиков прерываний BIOS написать резидентную программу, устанавливающую видеорежим и видеостраницу в соответствии с параметрами командной строки и отображающую информацию о параметрах текущего видеорежима в правом нижнем углу экрана.

Используя технику прямого доступа к видеопамяти написать программу, отображающую на экране текущую таблицу символов.

Не используя вызовов обработчиков прерываний BIOS написать программу, подменяющую стандартный обработчик прерываний от клавиатуры и отображающую на экране скан-коды нажимаемых клавиш. Обратить внимание на корректную обработку команды завершения работы программы.

Написать программу для рисования в окне терминала ДОС с помощью мыши различными цветами из заранее заданной палитры.

8.3.2. Перечень примерных вопросов для экзамена

- Устройство управления и арифметико-логическое 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.
- 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.
- Классификация прерываний. Аппаратные, программные, внешние, внутренние, маскируемые, немаскируемые, пошаговые, отладочные прерывания. Исключения и особенности их обработки. NMI и SMI. Обработчик прерывания.
- Общая схема подключения, алгоритм и режимы работы контроллера прерываний.

- Подключение внешних устройств к контроллеру прерываний. 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
- 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.
- 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.
- Статическая, динамическая, синхронная и асинхронная память.
- Регенерация памяти. Алгоритмы чтения и записи. Латентность, время доступа и время деактивации
- Механизм прямого доступа к памяти (DMA). Устройство и алгоритм работы контроллера DMA. Режимы работы и программирование.
- Системные шины и их характеристики. Пропускная способность. Протокол шины. Шина адреса. Шина данных. Шина управления. BUS-mastering.
- Шина ISA. Распределение ресурсов. Спецификация протокола ISA PnP. Протокол изоляции. Шина EISA.
- Архитектура шины PCI. Адресация устройств на шине. Обработка прерываний в системе с шиной PCI.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль ***Информационная безопасность***	**Код модуля** № 1140576/33630 УП 6938
Образовательная программа ***Информационная безопасность информационно-аналитических систем***	**Код ОП** ***10.05.04/01.01***
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки ***Информационная безопасность информационно-аналитических систем***	**Код направления и уровня подготовки** ***10.05.04***
Уровень подготовки ***специалист***	
ФГОС ВО ***Информационная безопасность информационно-аналитических систем***	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: № 1514 1 декабря 2016 г.

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Бакланов Валентин Викторович	к.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля С.В. Поршнев

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам.председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

1.1.Аннотация содержания дисциплины

В ходе изучения дисциплины рассматриваются общие принципы безопасности операционных систем на примере Windows, Linux, FreeBSD, Mac OS X. Студенты последовательно изучают механизмы защиты информации операционных систем на различных уровнях архитектуры, включая файловые системы, процедуры разграничения доступа компьютерных систем, управление учетных записей пользователя. Особое внимание уделено специфическим механизмам защиты обозначенных операционных систем, а также их администрированию и особенностям восстановления данных.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способностью анализировать физические явления и процессы, а также применять соответствующий математический аппарат при решении задач в сфере профессиональной деятельности (ОПК-1);
- способностью применять методы и средства обеспечения информационной безопасности специальных ИАС (ОПК-7).
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);
- способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС (ПК-10);
- способность разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности (ПК-11);
- способность разрабатывать программное и иные виды обеспечения специальных ИАС (ПК-12);
- способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности (ПК-13).

В результате освоения дисциплины студент должен:

Знать:

- угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии;
- основные принципы защиты компьютерной информации в операционных системах;
- виды и стратегии резервирования информации;
- программную архитектуру распространенных файловых систем FAT, NTFS, EXT*FS, UFS;
- методы исследования, поиска и восстановления информации на носителях с файловыми системами FAT, NTFS, EXT*FS, UFS;
- методику восстановления данных в поврежденных файловых системах и на поврежденных машинных носителях;
- механизмы защиты информации от несанкционированного доступа, встроенные в операционные системы Windows*, Linux, FreeBSD, Mac OS X;
- основные принципы администрирования операционных систем.

Уметь:

- выполнять функции администратора операционных систем;
- осуществлять планирование и создание учетных записей пользователей и рабочих групп, выполнять разграничение доступа к ресурсам компьютерных систем средствами ОС;
- производить основные настройки операционных систем, обеспечивающие требуемый уровень безопасности компьютерной информации;
- настраивать политику аудита, анализировать события, регистрируемые в журнальных файлах;
- настраивать сетевую инфраструктуру распространенных операционных систем;
- выполнять сбор информации о сетевом трафике, производить его анализ с целью оптимизации и обеспечения безопасности компьютерной сети;
- осуществлять управление сетевыми узлами с помощью средств системных служб и протокола SNMP;
- использовать стандартные сетевые утилиты операционных систем с целью диагностики и поиска неисправностей в сети;
- выполнять резервирование системной информации и данных;
- выполнять автоматическое и «ручное» восстановление системной информации, удаленных и испорченных данных;

Владеть (демонстрировать навыки и опыт деятельности):
- методами и средствами сбора информации о сетевом трафике;
- навыками защиты информационных систем;
- навыками настройки операционных систем.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	7
1.	**Аудиторные занятия**	68	68	68
2.	Лекции	34	34	34
3.	Практические занятия			
4.	Лабораторные работы	34	34	34
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	76	10,20	76
6.	**Промежуточная аттестация**	Эк.	2,33	Эк.
7.	**Общий объем по учебному плану, час.**	144	80,53	144
8.	**Общий объем по учебному плану, з.е.**	4		4

Ускоренная форма обучения (очно-заочная)

№	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего	В т.ч.	7

п/п		часов	контактная работа (час.)*	
1.	**Аудиторные занятия**	28	28	28
2.	Лекции	10	10	10
3.	Практические занятия	0	0	0
4.	Лабораторные работы	18	18	18
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	116	4,20	116
6.	**Промежуточная аттестация**	Эк.	2,33	Эк.
7.	**Общий объем по учебному плану, час.**	144	34,53	144
8.	**Общий объем по учебному плану, з.е.**	4		4

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Общие принципы безопасности операционных систем**	Ключевые элементы программной архитектуры операционных систем (ОС), определяющие защиту компьютерной информации и безопасность ЭВМ. Архитектура многозадачной сетевой операционной системы. Уровень ядра и уровень приложений. Объекты ядра. Аппаратно–зависимый программный слой. Защищенные файловые системы. Владение файловыми объектами и права доступа к ним. Изменение разрешений на доступ к файлам. Размещение элементов файловой системы на дисковом пространстве. Типовые файловые системы. Структура и назначение метаданных файлов. Понятие политики разграничения доступа в компьютерных системах. Одноуровневая и многоуровневая модели разграничения доступа, их достоинства и недостатки. Реализация технологии разграничения доступа в операционных системах. Модель безопасности и ее архитектура. Администрирование учетных записей пользователей. Группы пользователей. Права и привилегии пользователей и групп. Управление системной политикой безопасности. Стратегия предоставления прав на доступ к ресурсам. Хранение парольной информации. Алгоритм сетевой аутентификации. Обеспечение безопасности при удаленном доступе. Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС. Безопасность системных данных. Способы защиты системных файлов от незаконной модификации. Управление памятью. Механизмы виртуальной памяти. Создание и уничтожение процессов. Управление процессами и контроль над ними. Реализация многозадачного и многопоточного режимов. Механизмы системных вызовов. Защита на уровне межпроцессного взаимодействия. Сокрытие процессов. Реализация защитных требований на уровне командной оболочки. Защита программного обеспечения от незаконной модификации. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора.
2	**Защита компьютерной информации в операционных системах Linux и FreeBSD**	Ключевые элементы программной архитектуры ОС, влияющие на защиту информации. Базовые понятия. Основные отличия операционных систем Linux и FreeBSD. Файл как универсальный объект ОС. Виды файлов. Права доступа к файлам. Основные команды, позволяющие работать с файлами. Действия над обычными

		файлами: создание, копирование, перемещение, удаление. Работа с каталогами. Создание и изменение разрешений на доступ к файлам. Использование «жестких» и символических ссылок. Дополнительные атрибуты файлов, поддерживаемые в ОС Linux. Работа со специальными файлами устройств. Загрузчики операционных систем LILO, GRUB. Обеспечение защиты от НСД при загрузке ОС. Вход в систему в однопользовательском режиме. Загрузка ПК с LiveCD с целью устранения неполадок. Архитектура файловых систем ext*fs и ufs*. Размещение элементов файловой системы на дисковом пространстве. Назначение и структура суперблока, описателей групп блоков, карт битовых полей, индексных дескрипторов, журнала транзакций. Структура индексного дескриптора регулярного файла, каталога, символической ссылки. Работа с устройствами дисковой и полупроводниковой памяти. Создание, изменение и удаление дисковых разделов. Отображение информации о дисковых разделах и файловых системах. Форматирование разделов и создание файловых систем. Конфигурационный файл /etc/fstab. Монтирование устройств и дисковых разделов с различными файловыми системами. Размещение файловых систем на дисковом пространстве. Монтирование разделов памяти с различными файловыми системами. Установление дисковых квот. Восстановление логически удаленных или поврежденных файлов. Последовательность логического удаления файлов в файловых системах ext*fs и ufs*. Виды повреждений файловой системы. Утилиты для работы с поврежденными файловыми системами. Возможности дисковых редакторов типа Linux Disk Editor и отладчиков файловых систем для восстановления утерянной компьютерной информации. Особенности восстановления файлов в различных файловых системах. Использование записей из журнальных файлов. Блочное копирование информации с поврежденных машинных носителей с помощью утилиты dd. Ключевые аргументы командной строки. Сетевое копирование с использованием утилиты netcat. Атрибуты процесса. Файловая система /proc как «зеркало» процессов. Переменные окружения. Создание и уничтожение процессов, изменение их приоритетов. Способы автоматического запуска и остановки программ. Периодически запускаемые процессы. Запуск и остановка программ в интерактивном и фоновом режимах. Средства взаимодействия между процессами. Перенаправление ввода/вывода. Терминальный режим и консольные атаки. Вывод информации о процессах. Наблюдение за процессами и контроль производительности системы. Признаки камуфляжа несанкционированно выполняемых процессов. Программные возможности сокрытия процессов. Использование возможностей командных оболочек при решении штатных задач администрирования. Типовой синтаксис команд. Запуск программ в фоновом режиме. Запуск нескольких команд, в т.ч. по условию. Командные файлы. Перенаправление ввода и вывода. Конвейеры.

		Управление операционной системой в многотерминальном режиме. Работа с файловым менеджером Midnight Commander. Пользователи и их виды. Группы пользователей. Учетные записи пользователей и работа с ними. Изменение, редактирование, удаление и временное блокирование учетных записей. Конфигурационные файлы group, passwd, master.passwd, shadow, login.defs. Временные отметки и признаки паролей. Смена паролей. Процедура регистрации и ее безопасность. Смена пользователей. Предоставление эффективных прав доступа. Использование механизма SUDO. Практические задачи на разграничение доступа и их решения. Предоставление пользователям временных прав суперпользователя. Распространенные атаки на права администратора системы. Исследование учетных записей пользователей. Обнаружение неавторизованных учетных записей пользователей и групп. Копирование и запись данных. Архивация и резервирование. Сетевые возможности операционных систем. Контроль и настройка сетевых интерфейсов. Разведка узлов компьютерной сети и сетевых служб. Методы сканирования узлов ЛВС. Возможности утилиты nmap. Режимы открытого и скрытного сканирования. Перехват и анализ сетевого трафика с помощью утилиты tcpdump. Задание условий фильтрации трафика. Особенности настройки и проверки работоспособности узлов беспроводных сетей. Уязвимости алгоритмов криптографической защиты. Наблюдение и аудит в ОС Linux и FreeBSD. Сбор информации об опасных файловых объектах. Поиск необычных и скрытых файлов и каталогов. Наблюдение за процессами и пользователями. Отслеживание взаимосвязей между субъектами, процессами и объектами. Аудит событий и его безопасность. Системные протоколы, их расположение и заполнение. Источники, потребители и уровни значимости сообщений. Защита системы протоколирования событий. Основные ошибки и просчеты в администрировании компьютерных сетей под управлением операционных систем Linux и FreeBSD. Анализ настроек безопасности UNIX-систем.
3	**Защита компьютерной информации в операционных системах семейства Windows**	Реализация технологии разграничения доступа в ОС Windows *. Объекты и субъекты доступа. Права и методы доступа. Дескриптор защиты. Дискреционный список контроля доступа. Системный список контроля доступа. Структура маркера доступа. Процесс проверки подлинности при входе в систему. Стратегия предоставления прав на доступ к ресурсам. Защита данных средствами разрешений файловой системы NTFS. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows*. Методы идентификации и аутентификации пользователей, применяемые в ОС Windows*. Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS. Структура зашифрованного файла. Создание ключа и

		сертификата агента восстановления. Хранение парольной информации. Анализ уязвимости паролей пользователей. Алгоритмы локальной и сетевой аутентификации. Механизмы криптографической защиты данных на логических разделах и съемных носителях информации, реализованные в ОС Windows 7. Технология BitLocker. Создание замкнутой программной среды с помощью функции AppLocker. Организация файловой системы NTFS. Основные свойства файловой системы NTFS. Структура MFT. Стандартные атрибуты файлов и каталогов в NTFS. Основные операции над объектами файловой системы. Резидентные и нерезидентные атрибуты. Потоки. Структура каталогов. Размещение файловой системы на дисковом пространстве. Разграничение доступа в ОС Windows*. Планирование и создание учетных записей пользователей и рабочих групп. Разграничение доступа к ресурсам. Разрешения доступа к общим папкам. Получение доступа к пользовательским данным с правами администратора. Структура системного реестра ОС Windows*. Редактирование реестра. Разделы и настройки системного реестра, определяющие политику безопасности. Использование реестра для настройки параметров ОС. Утилиты администрирования реестра с интерфейсом командной строки. Анализ и настройка политики безопасности. Анализ параметров безопасности. Рекомендуемые права пользователей. Управление системной политикой безопасности. Политика учетных записей. Разработка шаблона политики безопасности. Анализ и настройка политики безопасности с применением шаблонов. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора. Настройки журнала аудита. Анализ и восстановление данных на логических разделах NTFS. Подключение машинных носителей с NTFS-разделами. Восстановление главной загрузочной записи. Восстановление таблицы разделов и загрузочного сектора. Приемы и программное обеспечение для «ручного» восстановления удаленных файлов на NTFS-разделах. Возможности автоматизированного восстановления удаленных файлов. Анализ сетевых служб Windows*. Анализ сетевых компьютеров с использованием стандартных сетевых команд. Анализ сетевых узлов с использованием программ-сканеров портов. Анализ возможности сетевого подключения к файловым ресурсам Windows*. Использование инструментальных средств аудита безопасности компьютерных систем.
4	**Особенности защиты компьютерной информации в операционной системе Mac OS X**	Создание, изменение и удаление учетных записей пользователей. Регистрация в системе и выход из нее. Включение и использование учетной записи суперпользователя **`root`**. Виды паролей: пароль учетной записи, пароль администратора, мастер-пароль, пароль суперпользователя. Выбор

		паролей с помощью **Password Assistant**. Пароли в виде «связки ключей». Сброс и обновление паролей. Аппаратный пароль **Firmware Password**. Работа с файлами. Надежное удаление файлов. Права доступа к файлам. Запрет изменений файлов. Особенности файловой системы **hfsplus**. Структура файлов. Восстановление поврежденных файлов. Использование механизма SUDO для предоставления пользователям дополнительных прав. Системные настройки безопасности. Шифрование пользовательских данных с помощью **FileVault**. Включение и выключение механизма шифрования. Недостатки режима шифрования. Контроль за режимом изоляции программной среды. Системная защита от вредоносных программ и сетевых атак. Загрузка операционной системы в однопользовательском режиме. Защита компьютеров Apple от непосредственного доступа. Экранная заставка. Контроль рабочего места с помощью видеорегистрации. Настройка средств сетевой защиты Mac OS X 10.6. Особенности регистрации системных событий. Расположение и безопасность журналов аудита.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 13
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Общие принципы безопасности операционных систем	**15**	**9**	4		5	6	3	1		2													3	1					
2	Защита компьютерной информации в операционных системах Linux и FreeBSD	**38**	**20**	10		10	18	9	4		5		4	1										5	1					
3	Защита компьютерной информации в операционных системах семейства Windows	**41**	**22**	10		12	19	10	3		7		4	1										5	1					
4	Особенности защиты компьютерной информации в операционной системе Mac OS X	**32**	**17**	10		7	15	6	3		3		4	1										5	1					
	Всего (час), без учета промежуточной аттестации:	**126**	**68**	**34**		**34**	58	23	6		17		12	12										**18**	**18**					
	Всего по дисциплине (час.):	**144**	**68**				**76**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

Ускоренная форма обучения (очно-заочная)

Объем модуля (зач.ед.): 13
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																		
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Общие принципы безопасности операционных систем	**18**	**4**	1		3	**14**	**7**	5		2													**5**	1					
2	Защита компьютерной информации в операционных системах Linux и FreeBSD	**19**	**8**	3		5	**29**	**11**	6		5		**10**	1										**8**	1					
3	Защита компьютерной информации в операционных системах семейства Windows	**40**	**9**	3		6	**31**	**13**	6		7		**10**	1										**8**	1					
4	Особенности защиты компьютерной информации в операционной системе Mac OS X	**33**	**7**	3		4	**26**	**8**	5		3		**10**	1										**8**	1					
	Всего (час), без учета промежуточной аттестации:	**126**	**28**	**10**		**18**	**98**	**39**	22		17		**30**	30										**29**	**29**					
	Всего по дисциплине (час.):	**144**	**28**				**116**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Очная форма обучения (учебный план №6028, Версии 3,4)

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Исследование файловых объектов с правами пользователя	3
1	2	Исследование архитектуры файловых систем ext*fs	2
2	3	Восстановление данных программными средствами ОС Linux	2
2	4	Исследование процессов в ОС Linux	2
2	5	Исследование сетевых возможностей ОС Linux	2
2	6	Исследование беспроводной сети WiFi под управлением ОС Linux	2
2	7	Наблюдение и аудит в ОС Linux	2
3	8	Основы администрирования ОС Windows *	2
3	9	Использование реестра для настройки параметров ОС Windows *	2
3	10	Ручное восстановление данных на разделах FAT и NTFS	2
3	11	Аудит событий безопасности ОС Windows	2
3	12	Применение стандартных механизмов защиты ОС Windows 7	2
3	13	Применение механизма защиты шифрования файлов в ОС Windows 7 с использованием шифрующей файловой системы EFS. Применение механизма защиты BitLocker.	2
4	14	Исследование защитных механизмов операционной системы Mac OS X 10.6	7
		Всего:	**34**

Ускоренная форма обучения (очно-заочная) (учебный план №6968, Версия 1)

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Исследование файловых объектов с правами пользователя	2
1	2	Исследование архитектуры файловых систем ext*fs	1
2	3	Восстановление данных программными средствами ОС Linux	1
2	4	Исследование процессов в ОС Linux	1
2	5	Исследование сетевых возможностей ОС Linux	1
2	6	Исследование беспроводной сети WiFi под управлением ОС Linux	1
2	7	Наблюдение и аудит в ОС Linux	1
3	8	Основы администрирования ОС Windows *	1
3	9	Использование реестра для настройки параметров ОС Windows *	1
3	10	Ручное восстановление данных на разделах FAT и NTFS	1
3	11	Аудит событий безопасности ОС Windows	1
3	12	Применение стандартных механизмов защиты ОС Windows 7	1
3	13	Применение механизма защиты шифрования файлов в ОС Windows 7 с использованием шифрующей файловой системы EFS. Применение механизма защиты BitLocker.	1
4	14	Исследование защитных механизмов операционной системы Mac OS X 10.6	4
		Всего:	**18**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Реализация политики разграничения доступа средствами ОС Linux.*
- *Настройка политики безопасности ОС Windows *.*
- *Настройка Родительского контроля в Mac OS X 10.6.*

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

- *Модель безопасности и ее архитектура.*
- *Ключевые элементы программной архитектуры ОС Linux, влияющие на защиту информации.*
- *Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows*.*
- *Системные настройки безопасности ОС Mac OS X.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
1.Общие принципы безопасности операционных систем				*	*							
2.Защита компьютерной информации в операционных системах Linux и FreeBSD					*							
3.Защита компьютерной информации в операционных системах семейства Windows				*								
4.Особенности защиты компьютерной информации в операционной системе Mac OS X				*								

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Олифер В. Г. Сетевые операционные системы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер .— 2-е изд. — Москва [и др.] : Питер, 2008 .— 669 с. 10 экз.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника" / П. Б. Хорев .— М.: Academia, 2005.— 256 с. 29 экз.

9.1.2.Дополнительная литература

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

9.2.Методические разработки

1. Синадский Н.И. Безопасность операционных систем. УМК, 2007. Метаданные ресурса №7029
2. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS: учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007 .— 136 с. 90 экз.

9.3.Программное обеспечение

ОС Linux, Windows, Mac OS X

9.4. Базы данных, информационно-справочные и поисковые системы

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

9.5.Электронные образовательные ресурсы

Не предусмотрено

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*7,1-7*	*20*
Домашняя работа №2	*7,1-15*	*20*
Домашняя работа №3	*7,1-15*	*20*
Контрольные работы №1-4	*7,1-15*	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение лабораторных работ	*7,1-15*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.
2. Методы и средства защиты информации в системах с проводными линиями. Типы проводных линий. Виды угроз, создаваемых проводными линиями. Оценка степени паразитных связей в линиях и уровней паразитных излучений, создаваемых проводными линиями.
3. Паразитные каналы утечки информации в телефонных системах и телефонных кабелях. Акустоэлектрические преобразования в телефонных аппаратах при опущенной трубке. Оценка уровней сигналов и уровней помех в телефонных линиях. Оценка реальности образования канала утечки. Защита от утечки с использованием диодных устройств типа «Гранит», «Корунд» и других. Особенности работы этих устройств в современных электронных аппаратах.
4. Применение генераторов шума для закрытия канала утечки за счет акустоэлектрического преобразования. Виды зашумления телефонных линий с целью закрытия каналов утечки информации.
5. Высокочастотное навязывание в телефонных системах. Механизмы взаимодействия акустического сигнала с высокочастотным сигналом навязывания. Оценка реальности канала утечки за счет высокочастотного навязывания. Оценка чувствительности метода.
6. Преднамеренно созданные каналы утечки по проводным линиям. Включение закладных устройств с передачей информации по проводам. Маскировка сигналов путем использования занятых проводных линий: радиотрансляционных сетей, телефонных линий, сетей электропитания и других. Возможности и методы

выделения сигналов в проводных линиях от помех. Компенсация помех. Адаптивные автокомпенсаторы.

7. Аппаратура выделения информации методом ВЧ навязывания, возможности и методы обеспечения высокой чувствительности. Меры борьбы с ВЧ навязыванием. Аппаратура контроля за утечкой информацией по каналам ВЧ навязывания.
8. Закладные устройства в системах с проводными коммуникациями. Устройства съема речевой информации в телефонных линиях. Методы подключения устройств. Использование диктофонов. Методы защиты от описанных закладных устройств. Аппаратура контроля и защиты от утечки информации по проводным линиям. Недостатки существующей аппаратуры.
9. Электрические характеристики и принцип работы городских телефонных линий. Возможные способы подключения закладных устройств к телефонным линиям. Количественные характеристики возмущений, вносимых закладными устройствами, и оценка возможности обнаружения закладных устройств. Примеры построения телефонных радио ретрансляторов (закладных устройств) с питанием от телефонных линий и оценка степени их влияния на параметры телефонных линий.
10. Методы защиты телефонных (и других проводных) линий от утечки информации через закладные устройства, параллельные телефоны и другими путями:
11. Способы реализации данных методов. Достоинства и недостатки. Проблемы реализации.
12. Применение фильтров для борьбы с утечкой информации по проводным линиям. Требования к характеристикам фильтров. Фильтры, предназначенные для защиты от утечки информации по сети 220 В. Особенность сетевых фильтров. Проектирование сетевых фильтров. Схемная реализация фильтров: независимые фазные фильтры; связанные фильтры. Реализация индуктивных и емкостных элементов сетевых фильтров. Ограничения, накладываемые на характеристики фильтров эксплуатационными требованиями.
13. Включение фильтров. Синфазные и противофазные сигналы и наводки в фильтрах. Заземление фильтров. Фильтры, предназначенные для защиты от мощных импульсных помех и преднамеренных воздействий. Меры защиты других проводных линий: провода пожарной и охранной сигнализаций, провода линий оповещения, городская трансляционная сеть, кабели компьютерных сетей, другие проводные линии.
14. Каналы утечки информации образованные электромагнитным излучением. Утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Виды каналов утечки за счет ПЭМИН. Основные средства (обработки конфиденциальной информации). Образование каналов утечки за счет наводок с основных средств на вспомогательные. Определение количественных характеристик цепей паразитных связей. Паразитные емкостная, индуктивная и связи.
15. Закладные устройства, использующие радиоканал. Средства индивидуальной радиосвязи: сотовые телефоны, бесшнуровые телефонные аппараты, пейджеры и другие.
16. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Возможности современной радиоэлектроники по построению закладных устройств.
17. Проблемы обнаружения и борьбы с закладными устройствами (ЗУ). Обеспечение энергетической скрытности (ЗУ). Потенциал радиоканала. Оценка эффективности антенн передатчиков и радиоприемников. Оценка минимальной мощности передатчиков (ЗУ). Оценка пороговой чувствительности радиоприемников.
18. Приборы для обнаружения электромагнитных излучений. Широкополосные индикаторы напряженности поля. Узкополосные сканирующие приемники.

Проблемы, связанные с их применением. Принцип построения названных приборов. Проблемы построения сканирующих приемников. Обеспечение высокой избирательности по паразитным каналам приема. Обеспечение высокой скорости обзора широкого частотного диапазона.

19. Методы обнаружения закладных устройств и паразитных излучений с применением широкополосных индикаторов и сканирующих приемников. Мониторинг эфира. Акустическая завязка. Акустическая локация. Корреляционная обработка принятых сигналов. Проблемы, возникающие при обнаружении закладных устройств.
20. Закладные устройства, использующие сложные сигналы. Возможности реализации таких устройств на современной элементной базе. Возможности обнаружения таких устройств. Направление построения аппаратуры для обнаружения излучений со сложными сигналами.
21. Построение радиоканалов передачи данных (сообщений) с цифровой обработкой сигналов и с использованием сложных широкополосных несущих. Возможности и примеры построения радиопередатчиков со сложными сигналами. Микросхемы XE1202, AD9850. Построение радиоприемников сложных сигналов: с псевдослучайной перестройкой частоты. Проблемы синхронизации.
22. 20. Возможности и примеры построения радиоприемников приема сложных сигналов с фазовой манипуляцией. Построение устройств обработки сигналов на регистрах сдвига (цифровые корреляторы и согласованные фильтры). Использование ПАВ устройств (согласованные фильтры и конвольверы). Проблемы синхронизации.
23. Методы защиты от утечки информации через закладные устройства, использующие радиоканал, и ПЭМИ. Экранирование. Эффективность экранирования высокочастотного электромагнитного излучения сплошным металлическим экраном. Влияние щелей и отверстий. Эффективность экранирования сетчатым экраном.
24. Активные методы защиты. Эффективность зашумления широкополосным шумовым излучением. Эффективность зашумления ультразвуком.
25. Организованные каналы утечки (съема) информации – закладные устройства. Закладные устройства с проводными каналами передачи. Использование проводов сети 220 В и других проводных линий. Закладные устройства с радиоканалом. Диапазоны частот, мощность передатчиков, виды модуляции, виды сигналов, используемые в закладных устройствах.
26. Определение количественных характеристик цепей паразитных связей. Паразитные емкостная, индуктивная связи. Определение уровней наводок через паразитную емкость между приборами и проводниками. Определение уровней наводок за счет контуров с током (взаимной индуктивности). Излучение случайных антенн – электрических и магнитных диполей.
27. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Магнитные экраны на низких частотах. Магнитные экраны на высокой частоте. Поверхностный эффект и токи Фуко. Соотношения и количественные показатели степени экранирования электростатических и магнитных экранов.
28. Борьба с утечкой информации по техническим каналам. Методы обнаружения утечки информации за счет побочных излучений и излучений закладных устройств. Широкополосные индикаторы напряженности поля. Проблемы их применения. Сканирующие узкополосные приемники. Требования к характеристикам. Тактика применения. Проблемы использования.
29. Защита информации от утечки в телефонных каналах связи. Каналы утечки информации: прямой перехват переговоров путем подключения к телефонной линии; утечка информации по линии при положенной трубке за счет микрофонного

эффекта и других акустоэлектрических преобразований; перехват информации при помощи закладных устройств (типы и способы подключения); перехват информации за счет высокочастотного навязывания. Методы борьбы с утечкой информации. Зашумление телефонной линии. Виды и способы зашумления.

30. Побочные электромагнитные излучения радиоэлектронных средств. Излучения гетеродинов радиоприемников. Излучения элементов компьютеров. Методика и аппаратура контроля уровня побочных излучений. Методика определения информативности побочных излучений.
31. Основные методы защиты информации техническими средствами. Охрана источников информации. Скрытие достоверной информации. Дезинформирование.
32. Методы локализации и обнаружения закладных устройств. Акустическое зондирование и определение дальности до закладного устройства. Корреляционная обработки акустических сигналов для локализации закладных устройств. Анализ уровня высших гармоник в излучении закладных устройств.
33. Нелинейные локаторы. Принцип действия. Проблемы применения.
34. Методика и аппаратура для измерения уровней наведенных сигналов из одних проводных линий в другие. Оценка (измерение) наведенных напряжений и токов в проводных линиях от электронных приборов (основных средств обработки конфиденциальной информации).
35. Методика и аппаратура наблюдения за радио излучениями в эфире с целью выявления каналов утечки информации за счет ПЭМИН и закладных устройств (мониторинг эфира). Требования к аппаратуре наблюдения. Обоснование возможности выявления каналов утечки информации. Характеристика возможностей поисковой программы «Филин».
36. Методика и аппаратура для измерения характеристик канала передачи сигналов по проводам сети 220 В. Проблемы, возникающие при использовании данного канала для передачи данных.
37. Методика измерения характеристик излучения проводных линий при помощи прибора ST 031P «Пирания». Приборы, необходимые для измерений. Сравнительные характеристики излучения проводных линий различных конструкций.
38. Методика измерения уровней излучения приборов и элементов приборов (например, печатных плат). Аппаратура, необходимая для проведения этих измерений.
39. Методика обнаружения и измерения уровней информативных паразитных излучений компьютеров. Методика оценки радиуса R2 (минимального расстояния до компьютера, на котором отношение сигнал/шум не превышает заданной величины). Аппаратура, с помощью которой можно сделать такие измерения.
40. Методика оценки эффективности зашумления паразитных излучений компьютера и зашумления излучения закладного устройства с радиоканалом. Аппаратура, необходимая для проведения измерений.
41. Методика определения мощности излучения закладных устройств и других источников. Экспериментальное определение дальности обнаружения излучения закладного устройства.
42. Поиск, локализация и обнаружение закладных устройств при помощи широкополосного индикатора напряженности поля «Пирания». Причины, ограничивающие возможности данного прибора. Пути его совершенствования.
43. Методика и аппаратура для наблюдения и измерения характеристик канала утечки информации за счет акусто-электрического преобразования в электронной аппаратуре. Измерение паразитной частотной модуляции, возникающей в генераторе сигналов.

44. Методика и аппаратура для оценки эффективности зашумления закладного устройства, включенного в телефонную линию, при использовании прибора КТЛ 400.
45. Характеристика методов обнаружения закладных устройств, включенных в телефонную линию, реализованных в приборе КТЛ 400 и других методов. Характеристика проблем, возникающих при решении данной задачи.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено