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
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

ПРОТИВОДЕЙСТВИЕ НЕПРЕДНАМЕРЕННОМУ РАСПРОСТРАНЕНИЮ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль *«Противодействие непреднамеренному распространению информации»*	**Код модуля** 1138306/32077 УП 5433, 6323
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП** 10.05.02/01.01
Траектория образовательной программы (ТОП)	*не предусмотрено*
Направление подготовки *Информационная безопасность телекоммуникационных систем*	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки *специалист*	
ФГОС ВО *Информационная безопасность телекоммуникационных систем*	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *16 ноября 2016 г. приказ № 1426*

Екатеринбург, 2017

Общая характеристика образовательной программы (далее – ОХОП) составлена авторами:

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

Руководитель модуля С.В. Поршнев

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**

1.1. Объем модуля, 9 з.е.

1.2. Аннотация содержания модуля

Целью модуля «Противодействие непреднамеренному распространению информации» является формирование у студентов навыков распознавания и предотвращение проникновения и защиты программных средств от внешних воздействий.

1. 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.	**(ВВ)** Безопасность программ и данных	10	17	17		34	74	зачет	108	3
2.	**(ВВ)** Защита целостности компьютерной информации	10	17	17		34	74	зачет	108	3
3.	**(ВВ)** Реагирование на компьютерные инциденты	10	17	17		34	74	зачет	108	3
Всего на освоение модуля			51	51		102	222		324	9

2. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	
3.2.	**Кореквизиты**	Безопасность программ и данных, Защита целостности компьютерной информации, Реагирование на компьютерные инциденты

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

3.1. Планируемые результаты освоения модуля и составляющие их компетенции

Код результата обучения	Результаты обучения	Компетенции, формируемые в рамках достижения результатов обучения
РО- 1	Способность эффективно общаться в межкультурной среде в устной и письменной форме с применением информационно-коммуникационных технологий, демонстрировать профессиональную, социальную ответственность на основе правовых и этических норм, работать в команде и организовывать работу малых коллективов, развивать свои духовные и физические качества	способностью 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 к самоорганизации и самообразованию (ОК-8)
РО-4	Способность осуществлять в рамках проектной деятельности проектирование защищённых инфотелекоммуникационных систем с учётом актуальных информационных угроз	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6) способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования (ПК-7) –

Код результата обучения	Результаты обучения	Компетенции, формируемые в рамках достижения результатов обучения
РО- 5	Способность обеспечивать в рамках эксплуатационной деятельности защищенность и функциональность инфотелекоммуникационных систем, производить их администрирование и профилактику работоспособности	способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14) способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-15) способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.5)
РО-6	Способность организовывать в рамках эксплуатационной деятельности технологическое и метрологическое обеспечение производства с использованием аппарата теории радиоэлектронных устройств и систем	применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи способностью применять положения теорий (ДК-6)

Код результата обучения	Результаты обучения	Компетенции, формируемые в рамках достижения результатов обучения
РО-7	Способность обеспечить в рамках эксплуатационной деятельности целостность и конфиденциальность информации, в том числе с использованием средств противодействия иностранным техническим разведкам	способностью применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3) способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПСК-10.1) способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты (ПСК-10.3) информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.5)

4.2.Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		Безопасность программ и данных, ,	Защита целостности компьютерной информации	Реагирование на компьютерные инциденты
	ОК5		*	
	ОК8	*		
	ОПК3			*
	ОПК5	*	*	
	ПК6	*		
	ПК7		*	
	ПК14	*	*	
	ПК15			*
	ПСК10.1			*
	ПСК10.3	*		
	ПСК10.5		*	

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

Не предусмотрено.

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:
Не предусмотрена

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 [*список*].
5.3.2.2. **Перечень примерных тем итоговых проектов по модулю** [*список*].

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

РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль *«Противодействие непреднамеренному распространению информации»*	**Код модуля** 1138306/32077 УП 5433, 6323
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП** 10.05.02/01.01
Траектория образовательной программы (ТОП)	*не предусмотрено*
Направление подготовки *Информационная безопасность телекоммуникационных систем*	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки *специалист*	
ФГОС ВО *Информационная безопасность телекоммуникационных систем*	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *16 ноября 2016 г. приказ № 1426*

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Синадский Николай Игоревич	к.т.н., доцент	Доцент	Кафедра алгебры и фундаментальной информатики	
2	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

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 ДИСЦИПЛИНЫ «РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению процесса управления и реагирования на инциденты информационной безопасности (ИБ).

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 положения теорий
- электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки
- сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3)
- способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПСК-10.1)
- способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации
- способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты (ПСК-10.3)
- информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.5)

В результате освоения дисциплины студент должен:

Знать:

- принципы построения системы управления инцидентами ИБ;
- современные подходы к управлению и расследованию инцидентов ИБ;
- основные российские и международные стандарты в сфере управления инцидентами ИБ;
- последовательность действий по реагированию на инциденты ИБ;

Уметь:

- осуществлять сбор технических данных с компонентов информационной инфраструктуры;
- выполнять поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению;
- организовывать наличие технических данных на этапах создания и эксплуатации информационной инфраструктуры;
- выполнять работы по восстановлению работоспособности информационных систем при реагировании на инциденты ИБ;

Владеть (демонстрировать навыки и опыт деятельности):

- техническими средствами и инструментами для сбора и обработки технических данных;
- методиками восстановления работоспособности информационных 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.)*	*9*
1.	**Аудиторные занятия**	34	34	34
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	74	5,20	74
6.	**Промежуточная аттестация**	4	0,25	Зачет(4)
7.	**Общий объем по учебному плану, час.**	108	39,45	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	**Управление инцидентами информационной безопасности**	Понятие инцидентов ИБ. Нормативная база в сфере управления инцидентами ИБ. Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ. Реагирование на инциденты ИБ. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
2	**Сбор и анализ технических данных при реагировании на инциденты**	Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ: сбор технических данных с компонентов информационной инфраструктуры; поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению; распространение (передача) выделенной и оформленной содержательной (семантической) информации; обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры. Сбор и фиксация информации об инцидентах ИБ: способ выявления инцидента ИБ; источник информации об инциденте ИБ; содержание информации об инциденте ИБ, полученной от источника; сценарий реализации инцидента ИБ; дата и время выявления инцидента ИБ; состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности; способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования; информация об операторе связи и провайдере сети Интернет. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем. Копирование протоколов (журналов) регистрации. Копирование сетевого трафика. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление. Структура протокола обработки технических данных. Технические средства и инструменты для сбора и обработки технических данных:

		технические средства выполнения криминалистической копии (создания образа) запоминающих устройств и содержимого оперативной памяти СВТ; технические средства получения данных операционных систем о сетевых конфигурациях, о сетевых соединениях, об открытых файлах, о запущенных процессах, об открытых сессиях доступа.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

Объем модуля (зач.ед.): 8
Объем дисциплины (зач.ед.): 3

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	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	Управление инцидентами информационной безопасности	**49**	**16**	8	8		**30**	**12**	6	6													**5**	1					
2	Сбор и анализ технических данных при реагировании на инциденты	**55**	**18**	9	9		**40**	**14**	7	7													**5**	1					
	Всего (час), без учета промежуточной аттестации:	**104**	**34**	**17**	**17**		**70**	**26**	**13**	**13**													**10**						
	Всего по дисциплине (час.):	**108**	**34**				**70**	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

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования	3
1	2	Копирование содержимого оперативной памяти СВТ и получение данных операционных систем	3
1	3	Копирование протоколов (журналов) регистрации	2
2	4	Копирование сетевого трафика	2
2	5	Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление	2
2	6	Программный инструментарий эксперта-криминалиста	2
2	7	Механизмы компьютерного следообразования	4
		Всего:	**17**

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

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

Контрольная работа №1. *Обработки технических данных в рамках реагирования*

на инциденты ИБ.

Контрольная работа №2. *Программный инструментарий эксперта-криминалиста.*

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)
Управление инцидентами информационной безопасности	*							*				
Сбор и анализ технических данных при реагировании на инциденты	*							*				

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. 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.

9.1.2. Дополнительная литература

1. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты : курс лекций : учеб. пособие для вузов / В. В. Бакланов .— Екатеринбург : Изд-во Уральского университета, 2007 .— 232 с. — (Приоритетный национальный проект "Образование") (Математика. Компьютерные науки) .— Библиогр.: с. 229-232 .— ISBN 5-7996-0259-5.
2. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ.

безопасность телекоммуникац. систем" / С. П. Расторгуев .— Москва : Академия, 2007 .— 188 с. ; 22 см .— (Высшее профессиональное образование, Информационная безопасность) .— Слов. терминов: с. 182-185. — Библиогр.: с. 180-181 (39 назв.). — Допущено в качестве учебного пособия. — ISBN 978-5-7695-3098-2.

9.2. Методические разработки

1. Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.

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

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

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 сеть Интернет.

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

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

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**
Контрольная работа №1	*10,1-17*	*50*
Контрольная работа №2	*10,1-17*	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 1,0**		
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**
Практические занятия	*10,1-17*	*100*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0,6		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 1**		
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 для контрольных работ

Контрольная работа №1.

1) *Опишите методы сбора технических данных с компонентов информационной инфраструктуры на инциденты ИБ;*

2) *Укажите способы выделения из собранных технических данных семантической информации на инциденты ИБ;*

Контрольная работа №2.

1) *Укажите методы криминалистического копирования энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования.*

2) *Укажите методы копирование содержимого оперативной памяти СВТ и получение данных операционных систем на инциденты ИБ.*

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

1. Понятие инцидентов ИБ.
2. Нормативная база в сфере управления инцидентами ИБ.
3. Система управления инцидентами ИБ.
4. Обработка событий и инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
7. Сбор технических данных с компонентов информационной инфраструктуры.
8. Поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению.
9. Распространение (передача) выделенной и оформленной содержательной (семантической) информации.
10. Обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры.

11. Сбор и фиксация информации об инцидентах ИБ.
12. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных.
13. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования.
14. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем.
15. Копирование протоколов (журналов) регистрации.
16. Копирование сетевого трафика.
17. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление.
18. Структура протокола обработки технических данных.
19. Технические средства и инструменты для сбора и обработки технических данных.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

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

БЕЗОПАСНОСТЬ ПРОГРАММ И ДАННЫХ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль *«Противодействие непреднамеренному распространению информации»*	**Код модуля** 1138306/32077 УП 5433, 6323
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП** 10.05.02/01.01
Траектория образовательной программы (ТОП)	*не предусмотрено*
Направление подготовки *Информационная безопасность телекоммуникационных систем*	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки *специалист*	
ФГОС ВО *Информационная безопасность телекоммуникационных систем*	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *16 ноября 2016 г. приказ № 1426*

Екатеринбург, 2017

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Поршнев С.В.	Д.т.н., проф.	Директор УНЦ ИБ	Учебно-научный центр «Информационная безопасность»	
2	Бакланов В.В.	К.т.н.,доцент	доцент	Учебно-научный центр «Информационная безопасность»	

Руководитель модуля С.В. Поршнев

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

Зам. 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

ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «Хранение, резервирование и восстановление компьютерной информации»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению подходов и принципов обеспечения защиты программ и данных. В дисциплине излагаются вопросы защиты информации, обрабатываемой в распространенных клиентских приложениях, защита информации, хранимой на машинных носителях, концепции безопасности баз данных, критерии и методы оценивания надежности механизмов защиты систем баз данных, особенности организации средств защиты в распределенных системах управления базами 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 к самоорганизации и самообразованию (ОК-8)
- способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6)
- способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14)

В результате освоения дисциплины студент должен:

Знать:

- основные средства защиты машинных носителей информации от непосредственного доступа;
- общие принципы построения программно-алгоритмических средств защиты информации в сложных клиентских приложениях;
- методы защиты компьютерной информации средствами СУБД.

Уметь:

- правильно использовать защитные механизмы, внедренные на прикладном программном уровне,
- оценивать и контролировать эффективность мер защиты;
- организовать защиту БД в различных СУБД.

Владеть (демонстрировать навыки и опыт деятельности):

- технологией организации защиты информации применительно к конкретным СУБД и базам данных;
- современными средствами защиты АС от несанкционированного доступа.

1.4.Объем дисциплины

Очная форма обучения

№	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего	В т.ч.	*3*

п/п		часов	контактная работа (час.)*	
1.	**Аудиторные занятия**	34	34	34
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	74	7,65	74
6.	**Промежуточная аттестация**	з	0,25	з
7.	**Общий объем по учебному плану, час.**	108	41,9	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	**Защита компьютерной информации, хранимой в долговременных устройствах памяти**	Понятия о физических принципах и стойкости запечатления компьютерной информации на внешних машинных носителях. Средства записи и считывания информации с машинных носителей. Параметры дисковых накопителей и магнитных носителей, особенности их эксплуатации. Оптические носители информации. Внешняя память на полупроводниковых структурах. Общесистемные и специализированные программные средства и методы логического и физического удаления компьютерной информации, оценка их эффективности. Программные способы удаления хранимой компьютерной информации. Аппаратные устройства мгновенного размагничивания магнитных носителей, их характеристики. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Существующие способы и средства реставрации удаленной компьютерной информации и восстановления поврежденных машинных носителей. Возможности аппаратно–программного комплекса PC–3000. Методы и средства восстановления работоспособности полупроводниковых носителей USB-Flash и хранимой на них информации.
2	**Резервирование и архивирование компьютерной информации**	Резервирование компьютерной информации как основная мера обеспечения ее сохранности. Порядок хранения и обновления архивных копий. Сравнительные характеристики программ-архиваторов. Виды архивирования. Восстановление системной информации, данных и программного обеспечения с резервных копий. Виды и стратегии резервирования. Использование стандартных средств резервирования системной информации и данных, программ-архиваторов. Устройства и носители, используемые для резервного копирования. Организация отказоустойчивых дисковых конфигураций (RAID). Создание зеркальных и дуплексных наборов. Чередование дисков с записью четности. Восстановление информации из зеркальных наборов и наборов с чередованием и контролем четности.
3	**Защита компьютерной информации на уровне клиентских программных приложений**	Защитные механизмы текстового процессора Microsoft Word. Характеристика офисного пакета как операционной среды для разработки текстовых, графических, табличных и иных документов. Механизмы образования технологического информационного мусора, способствующие утечке конфиденциальной информации. Информация,

		содержащаяся в «Свойствах» и скрытых полях документа. Документ Word как стегоконтейнер. Накопление «мусора» во фрагментах документов и шаблонов. Режим «быстрого сохранения» документов. Способы выявления и удаления скрытых и пользовательских данных. Защитные механизмы, реализованные в текстовом процессоре Word. Особенности формата документов и шаблонов. Структура файлов Office XML. Возможности восстановления поврежденных файлов. Уязвимости нового формата Microsoft Word. Шифрование содержимого документа. Ограничение прав пользователей на документы. Защита целостности документов. Использование цифровой подписи и недостатки в ее реализации. Возможности парольной защиты от изменения документа и доступа к встроенному программному коду. Особенности встроенной среды программирования VBA. Программные проекты, модули, процедуры и функции. Событийные процедуры. Автоисполняемые макросы. Приоритет запуска событийных процедур из различных программных модулей в документах и шаблонах. Реализация стандартной защиты от вирусов в макросах. Возможности использования офисных приложений для обработки конфиденциальной информации. Защитные механизмы браузера Microsoft Internet Explorer. Организация Web-протоколов. Структура гипертекстовых документов формата html, htt, hta, chm. Основные тэги гипертекстового файла. Механизмы вызова программ с помощью гиперссылок. Запуск активных компонентов из HTML-файла. Реализация атак на отказ в обслуживании. Вызов компонентов ActiveX с помощью тэгов HTML-файла. Компоненты, безопасные для инициализации и использования. Подкачка компонентов ActiveX с Web-серверов. Цифровая подпись компонентов. Типовые атаки на браузеры, связанные с внедрением и удаленным запуском опасных программных компонентов. Возможности выявления вредоносных активных компонентов на Web-сайтах.
4	**Средства обеспечения безопасности баз данных**	Средства идентификации и аутентификации объектов баз данных, Языковые средства разграничения доступа, концепция и реализация механизма ролей, организация аудита событий в системах баз данных. Средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и восстановления баз данных, технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

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

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 иноязр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Защита компьютерной информации, хранимой в долговременных устройствах памяти	24	12	4	4		12	12	4	8																			
2	Резервирование и архивирование компьютерной информации	24	12	4	4		12	12	4	8																			
3	Защита компьютерной информации на уровне клиентских программных приложений	36	12	4	4		24	12	4	8			12	1															
4	Средства обеспечения безопасности баз данных	28	15	5	5		13	13	5	8																			
	Всего (час), без учета промежуточной аттестации**:**	**104**	**51**	**17**	**17**		**38**	**41**	**17**	**24**			**12**	**12**															
	Всего по дисциплине (час.):	**108**	**34**				**53**	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

5 Не предусмотрено

5.1 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Анализ и восстановление данных на МНИ	4
2	2	Резервирование данных. RAID-массивы	4
3	3	Исследование защитных механизмов текстового процессора Microsoft Word	2
3	4	Исследование защитных механизмов браузера Microsoft Internet Explorer	2
4	5	Защитные механизмы СУБД	5
		Всего:	**17**

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Анализ и восстановление данных на МНИ*
- *Резервирование данных. RAID-массивы*
- *Исследование защитных механизмов текстового процессора Microsoft Word*
- *Исследование защитных механизмов браузера Microsoft Internet Explorer*
- *Защитные механизмы СУБД*

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 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)
Защита компьютерной информации, хранимой в долговременных устройствах памяти	*							*				
Резервирование и архивирование компьютерной информации	*							*				
Защита компьютерной информации на уровне клиентских программных приложений	*							*				
Средства обеспечения безопасности баз данных	*							*				

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. Андрончик А.Н. и др. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков; Под ред. Н.И.Синадского. – Екатеринбург: ГОУ ВПО УГТУ - УПИ, 2007. – 246 с. 90 экз.
2. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2011. – 160 с. URL:http://biblioclub.ru/index.php?page=book&id=275694>.

9.1.2. Дополнительная литература

3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации,

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (20.03.2018).

4. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285 (20.03.2018).
5. Хаулет, Т. Защитные средства с открытыми исходными текстами: Практическое руководство по защитны м приложениям : учебное пособие / Т. Хаулет ; пер. с англ. В. Галатенко, О. Труфанова ; под ред. В. Галатенко ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2007. - 608 с. : ил., табл., схем. - (Основы информационных технологий). - ISBN 978-5-94774-629-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233306 (20.03.2018).

9.2. Методические разработки

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — Ссылка .— 2008 .— в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.
2. Бакланов В. В. Программно-аппаратная защита информации / Бакланов В.В., Ваулин С.С., Синадский Н.И. — УМК . — 2007. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7232>.
3. Гайдамакин Н.А. Информационная безопасность АИС, баз и банков данных / Гайдамакин Н.А. — Ссылка .— 2008 .— Курс "Информационная безопасность АИС, баз и банков данных" является специальным курсом для специальности "Компьютерная безопасность". Излагаются методы и средства защиты информации для автоматизированных информационных систем, баз и банков данных. УМКД включает учебное пособие, программу дисциплины, вопросы для самоконтроля, методические указания, экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11055>.

9.3.Программное обеспечение

Операционные системы семейства MS Windows (лицензии по числу рабочих мест).

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

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

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-401. Персональные компьютеры – 8 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-403. Персональные компьютеры – 8 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

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

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**
Домашняя работа №1	*10,1-15*	*100*
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**
Отчет по практическим работам	*10,1-15*	*100*
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**
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

1. Цели, достигаемые использованием процедур уплотнения и архивации данных.
2. Методы сжатия с потерей информации. Особенности реализации, области применения.
3. Методы сжатия без потери информации. Особенности реализации, области применения.
4. Теоретические обратимые алгоритмы сжатия, Выходные структуры, сферы применения, эффективность использования.
5. Основные положения и порядок реализации алгоритма Хаффмана.
6. Базовые и дополнительные функции современных диспетчеров архивов.
7. Распределенный архив. Оптимальный режим работы с распределенными архивами.
8. Особенности процесса уплотнения машинных носителей информации.
9. Цели, достигаемые использованием процедур архивации и созданием резервных копий. Основные и дополнительные типы архивов.
10. Стратегии резервного копирования «Простая ротация», «Ханойская башня», «10 Наборов».
11. Основные средства восстановления системы ОС Windows XP. Контрольная точка восстановления.
12. Этапы автоматического восстановления системы ASR. Достоинства и недостатки средства ASR. Ограничения, налагаемые доступными программно-аппаратными средствами.
13. Программа Norton Ghost. Назначение, основные функциональные возможности.
14. Программа Acronis True Image. Назначение, основные функциональные возможности.
15. Основные причины образования в среде Word информационного «технологического мусора».

16. Организационные и технологические способы защиты конфиденциальной информации, обрабатываемой в среде Word, от случайного распространения.
17. Событийные процедуры и их использование во вредоносных макросах. Приоритеты исполнения событийных процедур, связанных с документами и шаблонами Word.
18. Основные механизмы вирусного инфицирования документов и шаблонов Word. Реализация защиты от вирусов в макросах в различных версиях Word.
19. Защита целостности программных проектов в документах и шаблонах Word.
20. Сравнительная эффективность средств программной защиты от внедрения и запуска вредоносных макросов.
21. Возможности визуального обнаружения вредоносного программного кода в программной среде и документах Word.
22. Основные уязвимости Web-протоколов, позволяющие внедрять и запускать программный код.
23. Механизмы доверительных отношений к компонентам ActiveX, зарегистрированным в операционной системе в качестве безопасных.
24. Организационные и технологические меры защиты браузеров от удаленных атак из Интернет.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

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

ЗАЩИТА ЦЕЛОСТНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль *«Противодействие непреднамеренному распространению информации»*	**Код модуля** 1138306/32077 УП 5433, 6323
Образовательная программа *Информационная безопасность телекоммуникационных систем*	**Код ОП** 10.05.02/01.01
Траектория образовательной программы (ТОП)	*не предусмотрено*
Направление подготовки *Информационная безопасность телекоммуникационных систем*	**Код направления и уровня подготовки** 10.05.04
Уровень подготовки *специалист*	
ФГОС ВО *Информационная безопасность телекоммуникационных систем*	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *16 ноября 2016 г. приказ № 1426*

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Синадский Николай Игоревич	к.т.н., доцент	Доцент	Кафедра алгебры и фундаментальной информатики	
2	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. 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 ДИСЦИПЛИНЫ «ЗАЩИТА ЦЕЛОСТНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

1.1.Аннотация содержания дисциплины

Дисциплина посвящена изучению защитных механизмов, реализованных в современных универсальных операционных системах Windows, Linux, FreeBSD, Mac OS X.

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 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)
- средств обеспечения информационной безопасности телекоммуникационных систем с учетом
- предъявляемых к ним требований качества обслуживания и качества функционирования (ПК-7)
- способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14)
- способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.5)
- способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты (ПСК-10.3)

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):
- профессиональной терминологией в области информационной безопасности;
- 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.)*	*1*
1.	**Аудиторные занятия**	34	34	34
2.	Лекции	17	17	17
3.	Практические занятия			
4.	Лабораторные работы	17	17	17
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	74	5,10	74
6.	**Промежуточная аттестация**	22	0,25	З, 4
7.	**Общий объем по учебному плану, час.**	108	39,35	
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 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. 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.): 6
Объем дисциплины (зач.ед.): 3

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	**22**	**8**	4		4	15	12	4		8													3	1					
2	Защита компьютерной информации в операционных системах Linux и FreeBSD	**60**	**9**	5		4	17	13	5		8													4	1					
3	Защита компьютерной информации в операционных системах семейства Windows	**62**	**8**	4		4	12	12	4		8																			
4	Особенности защиты компьютерной информации в операционной системе Mac OS X	**50**	**9**	4		5	26	14	4		10		1	1																
	Всего (час), без учета промежуточной аттестации:	**104**	**34**	**17**		**17**	70	57	35		22		12	12										**7**	**2**					
	Всего по дисциплине (час.):	**108**	**34**				**70**	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.)
		8 семестр	
1	1	Исследование файловых объектов с правами пользователя	1
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 Wi-Fi под управлением ОС Linux	1
2	7	Наблюдение и аудит в ОС Linux	1
3	8	Основы администрирования ОС Windows	1
		9 семестр	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	1
3	13	Применение механизма защиты шифрования файлов в ОС Windows с использованием шифрующей файловой системы EFS. Применение механизма защиты BitLocker.	2
4	14	Исследование защитных механизмов операционной системы Mac OS X	2
		Всего:	**17**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

1 семестр

Домашняя работа №1. *Реализация политики разграничения доступа средствами ОС Linux.*

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

1 семестр

Контрольная работа № 1. *Модель безопасности и ее архитектура.*

Контрольная работа № 2. *Ключевые элементы программной архитектуры ОС Linux, влияющие на защиту информации.*

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. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007. — 136 с. 90 экз.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.
3. Синицын С.В. Операционные системы : учебник для вузов / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин .— 3-е изд., стер. — Москва : Издательский центр "Академия", 2013 .— 296 с. 9 экз.

9.1.2. Дополнительная литература

1. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (20.03.2018).
2. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285 (20.03.2018).
3. Хаулет, Т. Защитные средства с открытыми исходными текстами: Практическое руководство по защитны м приложениям : учебное пособие / Т. Хаулет ; пер. с англ. В. Галатенко, О. Труфанова ; под ред. В. Галатенко ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2007. - 608 с. : ил., табл., схем. - (Основы информационных технологий). - ISBN 978-5-94774-629-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233306 (20.03.2018).
4. 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.
5. Пог.Д. Mac OS X Leopard. Основное руководство / Дэвид Пог ; [пер. с англ. С. Маккавеева] .— Санкт-Петербург ; Москва : Символ-Плюс, 2008 .— 880 с. 1 экз.
6. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с. 10 экз.
7. Робачевский А.М. Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский. — Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002. — 514 с. 9. экз.

9.2. Методические разработки

1. Синадский Н.И. Безопасность операционных систем. УМК, 2007. Метаданные ресурса №7029

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

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

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 сеть Интернет.

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

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

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**
1 семестр		
Домашняя работа	*10,1-17*	*30*
Контрольные работы №1	*10,1-17*	*35*
Контрольные работы №2	*10,1-17*	*35*
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	*10,1-17*	*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 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 задачи домашних работ

Домашняя работа №1. *Какое минимально необходимое разрешение необходимо иметь, чтобы просматривать атрибуты файла:*

Чтение,
Чтение и Выполнение,
Изменение?

8.3.3. Примерные задачи контрольных работ

Контрольная работа № 1.

Указать последовательность загрузки ПК:

MBR – BR – BIOS
BR – BIOS – MBR
BIOS – MBR – BR.

Контрольная работа № 2. *Каким образом* **с***одержимое NTFS-раздела отслеживается в:*

таблице расположения файлов — FAT
главной загрузочной записи — MBR
таблице разделов — PT
главной файловой таблице — MFT?

8.3.4. Перечень примерных вопросов для зачета

8 семестр

1. Понятие комплексной информационной защиты от несанкционированного доступа. Элементы защиты и их краткая характеристика.
2. Одноуровневая модель разграничения доступа, достоинства и недостатки.
3. Многоуровневая модель разграничения доступа, достоинства и недостатки.
4. Реализация технологии разграничения доступа в ОС Windows.
5. Понятие механизмов идентификации и аутентификации, их реализация в ОС Windows.
6. Хранение парольной информации в ОС Windows.
7. Уязвимости ОС Windows при возможном физическом доступе злоумышленника. Меры защиты.
8. Уязвимости парольной защиты ОС Windows. Меры защиты.
9. Алгоритм сетевой аутентификации в ОС Windows.
10. 2. Понятие об EFS в ОС Windows. Структура зашифрованного файла.

11. 3. Аудит в компьютерных системах. Цели, возможности.
12. 4. Файловая система FAT с точки зрения обеспечения информационной безопасности.
13. 5. Основные свойства файловой системы NTFS.
14. 6. Структура NTFS.
15. 7. Понятие об MFT. Структура записи в MFT.
16. 8. Организация резидентных файлов в NTFS. Возможность восстановления удаленных резидентных файлов.
17. Организация нерезидентных файлов в NTFS. Возможность восстановления удаленных нерезидентных файлов.
18. Реализация защиты компьютерной информации в файловых системах Linux. Особенности файловых систем EXT*FS.
19. Структура метаданных файловых систем EXT*FS и их размещение на дисковом пространстве. Права доступа. Работа с объектами файловой системы.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

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