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
«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль *Средства и методы защиты информации*	**Код модуля** № 1139519
Образовательная программа *Компьютерная безопасность*	**Код ОП 10.05.01/01.02** Учебный план № 5347 (версия 4)
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки *Компьютерная безопасность*	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки *Специалитет*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Программа модуля 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	Баранский Виталий Анатольевич	д.ф.-м.н., профессор	Профессор	Кафедра алгебры и фундаментальной информатики	

Руководитель модуля В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль В.А. Баранский

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ «СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

1.1. Объем модуля, 19 з.е.

1.2. Аннотация содержания модуля

Модуль «Средства и методы защиты информации» относится к базовой части образовательной программы 10.05.01/01.02 Компьютерная безопасность и предполагает получение студентами компетенций по установке, наладке, тестированию и обслуживанию современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем. В модуль входят следующие дисциплины: «Криптографические протоколы», «Защита программ и данных», «Программно-аппаратные средства обеспечения информационной безопасности», «Основы построения защищённых компьютерных сетей».

1. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Очная форма обучения
УП 5347 (версия 4)

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего			Час.	Зач. ед.
1.	**(Б)** Основы построения защищённых компьютерных сетей	10	51		51	102	150	Экз.18 час.	252	7
2.	**(Б)** Криптографические протоколы	9	17	17		34	74	Экз.18 час.	108	3
3.	**(Б)** Программно-аппаратные средства обеспечения информационной безопасности	9-10	68	51		119	133	Экз.36 час.	252	7
4.	**(Б)** Защита программ и данных	9	17	17		34	38	зачет, 4 час.	72	2
			153	**85**	**51**	**289**	**395**	**76**	**684**	**19**

Заочная форма обучения не предусмотрена

2. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	
3.2.	**Кореквизиты**	Защита программ и данных Криптографические протоколы Основы построения защищенных компьютерных сетей Программно-аппаратные средства обеспечения информационной безопасности

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

3.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	**Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля**	**Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля**	**Универсальные компетенции (УОК, УОПК, УПК), формируемые при освоении модуля для нескольких ОП**
10.05.01/01.02	РО-02. Способность применять основополагающие принципы и современные достижения физико-математических наук, математического описания и построения компьютерных систем, а также современные информационные технологии в разработке технологических решений с использованием программного кода.	ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.	
	РО-03 Способность осуществлять проектирование систем защиты информации с учётом актуальных информационных угроз и с	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные	

	использованием современных достижений науки и техники.	операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-7, способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем; ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.	
	РО-04 Способность обеспечивать защищенность и функциональность компьютерных систем, производить их администрирование и профилактику работоспособности.	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами	

		данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-17, способность-производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение; ПК-18, способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации; ДПК-5, способность восстанавливать работоспособность систем	

		защиты при сбоях и нарушении функционирования; ДПК-6, способность обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи.	
	РО-06 Способность осуществлять планирование работ по защите информации в компьютерных системах.	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ДПК-2, способность к разработке требований и критериев информационной безопасности, согласованных со стратегией развития предприятия.	
	РО-07 Способность проводить аудит и аттестацию объектов, обеспечивающих информационную безопасность, на соответствие требованиям государственных и/или корпоративных документов, а также устанавливать режим информационной безопасности на предприятии и контролировать его соблюдение.	ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ПК-11, способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации;	
	РО-08 Способность к разработке, анализу и обоснованию адекватности математических моделей процессов, возникающих при функционировании программно-аппаратных	ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ПК-5, способность	

	средств защиты информации, а также к разработке математических моделей для оценки безопасности компьютерных систем.	участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.1, способность разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных	

		математических методов защиты информации.	

4.2 Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ПК-4	ПК-5	ПК-6	ПК-7	ПК-8	ПК-10	ПК-11	ПК-17	ПК-18
1	**(Б)** Основы построения защищённых компьютерных сетей			*	*	*		*		
2	**(Б)** Криптографические протоколы	*			*	*				
3	**(Б)** Программно-аппаратные средства обеспечения информационной безопасности		*				*			*
4	**(Б)** Защита программ и данных						*		*	*
Дисциплины модуля		ПСК-2.1	ПСК-2.3	ПСК-2.4	ПСК-2.5	ПК-5	ДПК-6	ДПК-2		
1	**(Б)** Основы построения защищённых компьютерных сетей			*						
2	**(Б)** Криптографические протоколы	*	*					*		
3	**(Б)** Программно-аппаратные средства обеспечения информационной безопасности				*		*			
4	**(Б)** Защита программ и данных					*				

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю:
Не предусмотрен

5.2. Форма промежуточной аттестации по модулю:
Не предусмотрена.

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

ПРИЛОЖЕНИЕ 1

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

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

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

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ

АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю
Не предусмотрен
5.3.2.2. **Перечень примерных тем итоговых проектов по модулю**
Не предусмотрен.

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

ЗАЩИТА ПРОГРАММ И ДАННЫХ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Средства и методы защиты информации*	**Код модуля** № 1139519
Образовательная программа *Компьютерная безопасность*	**Код ОП 10.05.01/01.02** Учебный план № 5347 (версия 4)
Направление подготовки *Компьютерная безопасность*	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки *специалитет*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

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 В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ЗАЩИТА ПРОГРАММ И ДАННЫХ»

1.1.Аннотация содержания дисциплины

Дисциплина реализуется в составе базового модуля *Средства и методы защиты информации* образовательной программы 10.05.01/01.02 Компьютерная безопасность. Содержание дисциплины предусматривает изучение подходов и принципов обеспечения защиты программ и данных. В дисциплине излагаются вопросы защиты информации, обрабатываемой в распространенных клиентских приложениях, 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:

- ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПК-17, способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение;
- ПК-18, способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ДПК -5, способность восстанавливать работоспособность систем защиты при сбоях и нарушении функционирования;

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
УП 5347 (версия 4)

№ 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
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	34	5,1	34
6.	**Промежуточная аттестация**	4	0,25	Зачет(4)
7.	**Общий объем по учебному плану, час.**	72	39,35	72
8.	**Общий объем по учебному плану, з.е.**	2		2

Заочная форма обучения не предусмотрена

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.): 19
Объем дисциплины (зач.ед.): 2

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод 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	17	8	4	4		9	3	1	2			6	1															
2	Резервирование и архивирование компьютерной информации	17	8	4	4		9	3	1	2			6	1															
3	Защита компьютерной информации на уровне клиентских программных приложений	17	8	4	4		9	3	1	2			6	1															
4	Средства обеспечения безопасности баз данных	17	10	5	5		7	3	1	2			4	1															
	Всего (час), без учета промежуточной аттестации:	**68**	**34**	**17**	**17**		**34**	**12**	**4**	**8**			**22**	**22**															
	Всего по дисциплине (час.):	**72**	**34**				**38**	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	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 Oracle	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*

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. 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. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем" / Н. А. Гайдамакин. — Москва :

Гелиос АРВ, 2002. — 368 с. : ил. ; 20 см .— Библиогр.: с. 354-355 (34 назв.). — допущено в качестве учебного пособия .— ISBN 5854380358 : 90.00.

9.1.2. Дополнительная литература

1. Гультяев А.К. Восстановление данных / А. К. Гультяев. — 2-е изд. — СПб. : Питер, 2006 .— 379 с.

9.2. Методические разработки

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 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. — 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	*9,1-15*	*25*
Домашняя работа №2	*9,1-15*	*25*
Домашняя работа №3	*9,1-15*	*25*
Домашняя работа №4	*9,1-15*	*25*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям –зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий –0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практическое занятие №1	*9,1-15*	*10*
Практическое занятие №2	*9,1-15*	*10*
Практическое занятие №3	*9,1-15*	*20*
Практическое занятие №4	*9,1-15*	*20*
Практическое занятие №5	*9,1-15*	*20*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

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

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

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

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

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

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

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

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

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

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

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач,	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач,

	выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

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

НТК по дисциплине не проводится

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 для домашних работ

Домашняя работа №1.

1) *Какими средствами файловой системы реализуются списки контроля доступа в ОС Windows:*

1) FAT16
2) FAT32
3) HPFS
4) NTFS
5) NWFS?

Обоснуйте свой выбор.

2) *Из чего состоит Файл в NTFS?:*

1) набор атрибутов, один из которых является данными
2) хранилище двоичных или текстовых данных
3) битовая карта
4) хранилище информации о его физическом расположении

Обоснуйте свой выбор.

Домашняя работа №2.

1) *В домене удалили учетную запись пользователя. Как можно прочитать файлы, созданные и зашифрованные им?*

1) скопировать файлы на раздел FAT
2) создать удаленную учетную запись заново и, зарегистрировавшись от ее имени, получить доступ к файлам
3) передать файлы лицу, являющемуся агентом восстановления
4) это сделать невозможно

Обоснуйте свой выбор.

2) Как описывается структура NTFS-раздела в:

1) таблице расположения файлов — FAT
2) главной загрузочной записи — MBR
3) таблице разделов — PT
4) главной файловой таблице — MFT.

Домашняя работа №3.

1) *При шифровании файла средствами EFS каким образом шифруются его данные?*

1) открытым ключом пользователя
2) личным ключом пользователя
3) случайно генерируемым ключом
4) ключом восстановления
5) открытым ключом пользователя и открытым ключом агента восстановления

2) *Какая последовательность загрузки персонального компьютера является корректной?*

1) MBR – BR – BIOS
2) BR – BIOS – MBR
3) BIOS – MBR – BR
4) MBR – BIOS – BR
5) BIOS – BR – MBR

Обоснуйте свой выбор.

Домашняя работа №4.

1) *В каком каталоге хранится секретный ключ пользователя для шифрования в файловой системе EFS?*

1) \Microsoft\SystemCertificates\My\Certificates
2) \Microsoft\Crypto\RSA \Идентификатор пользователя
3) \Microsoft\Protect\ Идентификатор пользователя
4) \Microsoft\ Идентификатор пользователя

Обоснуйте свой выбор.

2) В каком каталоге хранится файл блокировки для шифрования в файловой системе EFS?

1) \Microsoft\SystemCertificates\My\Certificates
2) \Microsoft\Crypto\RSA \Идентификатор пользователя
3) \Microsoft\Protect\ Идентификатор пользователя
4) \Microsoft\ Идентификатор пользователя

Обоснуйте свой выбор.

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

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Средства и методы защиты информации*	**Код модуля** № 1139519
Образовательная программа *Компьютерная безопасность*	**Код ОП 10.05.01/01.02** Учебный план № 5347 (версия 4)
Направление подготовки *Компьютерная безопасность*	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки *специалитет*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Попов Владимир Юрьевич	д.ф.-м.н., доцент	Профессор	Кафедра алгебры и фундаментальной информатики	

Руководитель модуля В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных

Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

1.1.Аннотация содержания дисциплины

Дисциплина реализуется в составе базового модуля *Средства и методы защиты информации* образовательной программы 10.05.01/01.02 Компьютерная безопасность. Содержание дисциплины предусматривает изучение основных типов криптографических протоколов и механизмов защиты информации с использованием криптографических протоколов.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

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

- ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;
- ПК-7, способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем;
- ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;
- ПСК-2.1, способность разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;
- ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;
- ДПК-2, способность к разработке требований и критериев информационной безопасности, согласованных со стратегией развития предприятия.

В результате освоения дисциплины студент должен:

Знать:

- классификацию и общую характеристику основных типов криптографических протоколов;
- основные принципы построения криптографических протоколов;
- особенности реализации криптографических протоколов.

Уметь:

- применять механизмы защиты, реализующие криптографические протоколы;
- оценивать и контролировать эффективность криптографических протоколов;
- разрабатывать компоненты криптографических протоколов.

Владеть (демонстрировать навыки и опыт деятельности):

- методикой разработки и применения криптографических протоколов.

1.4.Объем дисциплины

Очная форма обучения
УП 5347 (версия 4)

№ 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
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	56	5,1	56
6.	**Промежуточная аттестация**	18	2,33	Э(18)
7.	**Общий объем по учебному плану, час.**	108	41,43	108
8.	**Общий объем по учебному плану, з.е.**	3		3

Заочная форма обучения не предусмотрена

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Введение в криптографические протоколы**	Общие сведения о криптографических протоколах. Принципы построения криптографических протоколов. Классификация криптографических протоколов. Методы анализа надежности криптографических протоколов.
2	**Идентификация и аутентификация**	Типы протоколов идентификации и аутентификации. Методы интегрирования протоколов идентификации и аутентификации в компьютерные системы.
3	**Протоколы для работы с ключами**	Протоколы обмена ключами. Депонирование ключей и возможность контроля информационного взаимодействия.
4	**Протоколы хранения информации**	Схемы разделения секрета. Доказательство с нулевым разглашением.
5	**Сетевые протоколы**	Протоколы широковещания. Системы электронного голосования. Протоколы защиты данных в сети Internet.
6	**Графические методы теории криптографических протоколов**	Использование графических элементов в сложных многофункциональных протоколах. Визуальные протоколы. Протоколы обмена информацией под наблюдением.
7	**Интеллектуальные методы теории криптографических протоколов**	Нейросетевые протоколы. Протоколы на основе генетических алгоритмов. Использование

		интеллектуальных методов при построении и анализе криптографических протоколов. Протоколы квантовой и постквантовой криптографии.
8	**Эзотерические протоколы**	Типы эзотерических протоколов. Методы построения и анализа криптографических протоколов.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

Объем модуля (зач.ед.): 19
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязыч. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Введение в криптографические протоколы	13	6	3	3		7	2	1	1			5	1																
2	Идентификация и аутентификация	11	4	2	2		7	2	1	1			5	1																
3	Протоколы для работы с ключами	11	4	2	2		7	2	1	1			5	1																
4	Протоколы хранения информации	11	4	2	2		7	2	1	1			5	1																
5	Сетевые протоколы	11	4	2	2		7	2	1	1			5	1																
6	Графические методы теории криптографических протоколов	11	4	2	2		7	2	1	1			5	1																
7	Интеллектуальные методы теории криптографических протоколов	11	4	2	2		7	2	1	1			5	1																
8	Эзотерические протоколы	11	4	2	2		7	2	1	1			5	1																
	Всего (час), без учета промежуточной аттестации:	**90**	**34**	**17**	**17**		**56**	**16**	**6**	**6**			**40**	**40**																
	Всего по дисциплине (час.):	**108**	**34**				**74**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

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

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Введение в криптографические протоколы	3
2	2	Идентификация и аутентификация	2
3	3	Протоколы для работы с ключами	2
4	4	Протоколы хранения информации	2
5	5	Сетевые протоколы	2
6	6	Графические методы теории криптографических протоколов	2
7	7	Интеллектуальные методы теории криптографических протоколов	2
8	8	Эзотерические протоколы	2
Всего:			17

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Анализ надежности многофункианального криптографического протокола*
- *Программирование протоколов идентификации и аутентификации*
- *Программирование протоколов для работы с ключами*
- *Программирование протоколов хранения информации*
- *Программирование сетевых протоколов*
- *Программирование графических протоколов*
- *Программирование протоколов постквантовой криптографии*
- *Программирование эзотерических протоколов*

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)
Введение в криптографические протоколы	*											
Идентификация и аутентификация	*											
Протоколы для работы с ключами	*											
Протоколы хранения информации	*											
Сетевые протоколы	*											
Графические методы теории криптографических протоколов	*											
Интеллектуальные методы теории криптографических протоколов	*											
Эзотерические протоколы	*											

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. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер ; [пер. с англ. Н. Н. Селиной под ред. А. В. Журавлева] .— Москва ; Санкт-Петербург ; Киев : Диалектика, 2005 .— 424 с. ; 24 см .— Предм. указ.: с. 418-421. — Пер. изд.: Practical Cryptography / N. Ferguson, B. Schneier. - 2003. — Библиогр.: с. 410-417.

9.1.2. Дополнительная литература

2. Введение в криптографию : Учебник / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др. ; Под общ. ред. В.В. Ященко .— СПб.; М.; Харьков; Минск : МЦНМО : Питер, 2001 .— 288 с. : ил. ; 24 см .— (Новые математические дисциплины) .— Библиогр. в конце гл. — Прил.: Отрывок из ст. К. Шеннона "Теория связи в секретных системах": с. 251-287. — без грифа .— ISBN 5-318-00443-1 : 80.00.

9.2. Методические разработки

Отсутствуют

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://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ
   http://study.ustu.ru/info/default.aspx

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Не предусмотрено

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	*9,1-15*	*20*
Домашняя работа №2	*9,1-15*	*10*
Домашняя работа №3	*9,1-15*	*10*
Домашняя работа №4	*9,1-15*	*10*
Домашняя работа №5	*9,1-15*	*10*

Домашняя работа №6	*9,1-15*	*10*
Домашняя работа №7	*9,1-15*	*10*
Домашняя работа №8	*9,1-15*	*20*
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 –0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практическое занятие №1	*9,1-15*	*20*
Практическое занятие №2	*9,1-15*	*10*
Практическое занятие №3	*9,1-15*	*10*
Практическое занятие №4	*9,1-15*	*10*
Практическое занятие №5	*9,1-15*	*10*
Практическое занятие №6	*9,1-15*	*10*
Практическое занятие №7	*9,1-15*	*10*
Практическое занятие №8	*9,1-15*	*20*
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		
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	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность,

		активность.	творческий подход.

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

НТК по дисциплине не проводится.

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 составе домашних работ

Домашняя работа №1. *Обосновать размер ключа в криптоалгоритме ГОСТ 28147-89:*

- 64 бит
- 128 бит
- 256 бит
- 512 бит
- произвольный

Домашняя работа №2. *В чем состоит проблема распространения ключей при использовании криптосхемы:*

- асимметричной
- симметричной
- гибридной
- возникает при всех вышеуказанных схемах
- такой проблемы нет?

Домашняя работа №3. *В чем состоит процесс преобразования открытых данных в закрытые с помощью шифра:*

- зашифрование
- дешифрование
- расшифрование
- стеганоанализ
- криптоанализ

Домашняя работа №4. *В какой криптосхеме принцип «зашифровать может любой, расшифровать — только тот, кто знает секретный ключ» используется:*

- асимметричной
- симметричной
- ЭЦП
- хэш-функции
- в любой системе шифрования?

Ответ обосновать.

Домашняя работа №5. *Какой из алгоритмов шифрования является алгоритмом с открытым ключом:*

- DES
- ГОСТ 28147-89
- ГОСТ Р 34.12-2015
- AES

RSA?
Ответ обосновать.

Домашняя работа №6. *Какая из систем предусматривает три режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки:*

— IDEA
— RSA
— ГОСТ 28147-89
— RC2 или RC4
DES?
Ответ обосновать.

Домашняя работа №7. Любая ли криптографическая система основана на использовании:

— криптографических ключей
— разомкнутых линий
— односторонних функций
— методов сокрытия информации
— зашифрованных виртуальных дисков?
Ответ обосновать.

Домашняя работа №8. *Используют ли в симметричной криптосистеме отправитель и получатель сообщения:*

— один и тот же секретный ключ
— ключи, получаемые в результате взаимного обмена
— различные секретные ключи
— различные открытые ключи
— вообще не используют ключей?
Ответ обосновать.

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Общие сведения о криптографических протоколах.
2. Принципы построения криптографических протоколов.
3. Классификация криптографических протоколов.
4. Методы анализа надежности криптографических протоколов.
5. Типы протоколов идентификации и аутентификации.
6. Методы интегрирования протоколов идентификации и аутентификации в компьютерные системы.
7. Протоколы обмена ключами.
8. Депонирование ключей и возможность контроля информационного взаимодействия.
9. Схемы разделения секрета.
10. Доказательство с нулевым разглашением.
11. Протоколы широковещания.
12. Системы электронного голосования.

13. Протоколы защиты данных в сети Internet.
14. Использование графических элементов в сложных многофункциональных протоколах.
15. Визуальные протоколы.
16. Протоколы обмена информацией под наблюдением.
17. Нейросетевые протоколы.
18. Протоколы на основе генетических алгоритмов.
19. Использование интеллектуальных методов при построении и анализе криптографических протоколов.
20. Протоколы квантовой и постквантовой криптографии.
21. Типы эзотерических протоколов.

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

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Средства и методы защиты информации*	**Код модуля** № 1139519
Образовательная программа *Компьютерная безопасность*	**Код ОП 10.05.01/01.02** Учебный план № 5347 (версия 4)
Направление подготовки *Компьютерная безопасность*	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки *специалитет*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

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 В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ»

1.1.Аннотация содержания дисциплины

Дисциплина реализуется в составе базового модуля *Средства и методы защиты информации* образовательной программы 10.05.01/01.02 Компьютерная безопасность. Содержание дисциплины предусматривает изучение подходов и принципов проектирования защищенных компьютерных сетей. В дисциплине излагаются способы реализации основных механизмов защиты компьютерных сетей на программном уровне.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

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

- ПК-6, способность участвовать в разработке проектной и технической документации;
- ПК-7, способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем;
- ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;
- ПК-11, способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации;
- ПСК-2.4, способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

В результате освоения дисциплины студент должен:

Знать:

- методы защиты компьютерной информации;
- классификацию и общую характеристику программно-аппаратных средств защиты информации;
- основные принципы построения защищенных компьютерных систем;
- особенности реализации методов защиты информации программно-аппаратными средствами.

Уметь:

- применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем;
- оценивать и контролировать эффективность мер защиты;
- разрабатывать компоненты программно-аппаратных комплексов защиты информации.

Владеть (демонстрировать навыки и опыт деятельности):

- методикой проектирования систем защиты информации от несанкционированного доступа.

1.4.Объем дисциплины

Очная форма обучения

УП 5347 (версия 4)

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*10*
1.	**Аудиторные занятия**	102		102
2.	Лекции	51	51	51
3.	Практические занятия			
4.	Лабораторные работы	51	51	51
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	132	15,3	132
6.	**Промежуточная аттестация**	18	2,33	Э (18)
7.	**Общий объем по учебному плану, час.**	252	119,63	252
8.	**Общий объем по учебному плану, з.е.**	7		7

Заочная форма обучения не предусмотрена

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Методология оценки безопасности информационных технологий**	Основные подходы к проектированию защищенных телекоммуникационных систем. Структура ГОСТ Р ИСО/МЭК 15408. Методология оценки безопасности информационных технологий. Контекст безопасности. Подход общих критериев. Понятия безопасности. Описательные возможности общих критериев. Виды оценок. Поддержка доверия. Виды требований безопасности (функциональные и доверия). Профиль защиты. Профиль защиты «Клиентская операционная система». Среда безопасности. Цели безопасности. Функциональные требования. Требования доверия. Описание объекта оценки. Среда безопасности объекта оценки. Требования безопасности информационных технологий. Функции безопасности объекта оценки. Логическое обоснование целей и требований безопасности.
2	**Проектирование подсистем защиты информации от несанкционированного доступа**	Функциональная схема комплексной системы защиты информации. Модель управления доступом к защищаемым ресурсам. Проектирование подсистем идентификации и аутентификации на основе носителей ключевой информации. Общие принципы реализации механизмов разграничения прав доступа. Практическая реализация подсистемы управления доступа к каталогам. Состав и реализация диспетчера доступа к ресурсам. Непротиворечивые правила назначения (изменения) прав доступа. Формальная модель диспетчера доступа. Функциональная схема системы защиты, реализующая механизм уровневого контроля списков санкционированных событий. Алгоритм контроля доступа пользователя к ресурсам защищаемого объекта. Реализация механизма обеспечения замкнутости программной среды. Механизмы контроля целостности информации и их реализация. Механизмы аудита событий и их реализация. Технология доверенной загрузки операционной системы. Структура программно-аппаратного комплекса защиты загрузки операционной системы. Разработка программного компонента идентификации и аутентификации пользователей, функционирующего до загрузки операционной системы. Структура программы начальной загрузки. Программирование загрузчика персонального компьютера. Применение технологии виртуальных машин для тестирования разрабатываемого

		компонента идентификации и аутентификации.
3	**Проектирование подсистем криптографической защиты информации**	Разработка интерфейсной части системы криптографической защиты информации на основе библиотек, предоставляемых криптопровайдером. Реализация функций шифрования, подписывания и проверки электронно-цифровой подписи с использованием алгоритмов RSA, ГОСТ Р34.10-94 и ГОСТ 28147-89. Порядок взаимодействия приложений с криптографическими модулями операционной системы на базе Microsoft Cryptographic Application Programming Interface (MS Crypto API). Особенности проектирования интерфейса пользователя для генерации ключевой информации на основе клавиатурного ввода, записи и извлечения ключей на носители, гарантированного уничтожения файлов. Реализация функций шифрования (зашифрования, расшифрования, подписывания, проверки подписи) файлов по выбору в компилирующей визуальной среде разработки прикладных программ Delphi. Реализация Windows-подобного интерфейса пользователя для генерации ключевой информации на основе клавиатурного ввода, записи ключа на ключевой носитель. Разработка руководства пользователя программы криптографической защиты информации. Разработка системы защищенного документооборота на базе программно-аппаратного комплекса, реализующего подсистему криптографической защиты информации. Архитектура системы защищенного документооборота. Структура и функции удостоверяющего центра. Установка и конфигурация компонентов удостоверяющего центра. Выпуск сертификатов пользователей. Настройка клиентов системы защищенного документооборота.
4	**Проектирование подсистем обнаружения компьютерных атак**	Технология интеллектуальных многоагентных систем. Понятие агентов защиты. Архитектура многоагентных систем. Агентно-ориентированная система моделирования атак, многоагентная система обнаружения вторжений. Спецификация «системного ядра» многоагентной системы. Проектирование компонентов многоагентной СОА. Разработка сенсоров различного типа. Протоколы информирования о событиях, зафиксированных сенсором. Методологии обнаружения атак: простой поиск по шаблону, поиск по шаблону с сохранением состояния, разбор протоколов, эвристический анализ, обнаружение аномалий, анализ соответствия политике безопасности. Основные математические методы, лежащие в основе обнаружения аномалий, и их реализации в СОА. Модель системы корреляции событий информационной безопасности

5	**Проектирование защищенных автоматизированных информационных систем**	Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах
6	**Проектирование средств защиты информации от несанкционированного распространения**	Общие принципы построения подсистем защиты от несанкционированного распространения программного обеспечения на основе электронных ключей Guardant Использование электронных ключей Guardant для защиты приложений

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

Объем модуля (зач.ед.): 19
Объем дисциплины (зач.ед.): 7

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 иноя. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Методология оценки безопасности информационных технологий	36	14	7		7	22	14	7		7		8	1															
2	Проектирование подсистем защиты информации от несанкционированного доступа	40	18	8		8	22	14	7		7		8	1															
3	Проектирование подсистем криптографической защиты информации	36	14	7		7	22	14	7		7		8	1															
4	Проектирование подсистем обнаружения компьютерных атак	48	26	13		13	22	14	7		7		8	1															
5	Проектирование защищенных автоматизированных информационных систем	42	20	10		10	22	14	7		7		8	1															
6	Проектирование средств защиты информации от несанкционированного распространения	32	10	6		6	22	14	7		7		8	1															
	Всего (час), без учета промежуточной аттестации:	**234**	**102**	**51**		**51**	**132**	**84**	**42**		**42**		**48**	**48**															
	Всего по дисциплине (час.):	**252**	**102**				**150**	В т.ч. промежуточная аттестация																		**0**	**18**	**0**	**0**

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

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Программирование подсистемы аутентификации пользователей на основе носителей ключевой информации типа Touch Memory	2
1	2	Программирование прототипа подсистемы управления доступа к каталогам	2
1	3	Программирование модуля, реализующего дополнительный механизм аудита событий безопасности в ОС Windows	3
2	4	Программирование компонента идентификации и аутентификации пользователей, функционирующего до загрузки операционной системы	4
2	5	Реализация Windows-подобного интерфейса пользователя для генерации ключевой информации на основе клавиатурного ввода	4
3	6	Реализация функций шифрования (зашифрования, расшифрования, подписывания, проверки подписи) файлов по выбору с использованием библиотеки Крипто-Про CSP	3
3	7	Проектирование средств криптографической защиты информации на базе библиотек СКЗИ «Верба-OW»	4
4	8	Проектирование сенсоров СОА	4
4	9	Интеграция сенсоров в состав многоагентной системы обнаружения атак	4
4	10	Математические методы, лежащие в основе обнаружения аномалий, и их реализации в СОА	5
5	11	Применение библиотек CryptoPro.Sharpei для работы с СКЗИ «КриптоПро CSP» на базе платформы программирования Microsoft .Net Framework	5
5	12	Проектирование VPN на базе средств криптографической защиты информации «КриптоПро CSP» и «Верба-OW»	5
6	13	Использование электронных ключей Guardant для защиты приложений	6
		Всего:	**51**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Программирование подсистемы аутентификации пользователей на основе носителей ключевой информации типа Touch Memory*
- *Программирование прототипа подсистемы управления доступа к каталогам*
- *Программирование компонента идентификации и аутентификации пользователей, функционирующего до загрузки операционной системы*
- *Проектирование средств криптографической защиты информации на базе библиотек СКЗИ «Верба-OW»*
- *Проектирование VPN на базе средств криптографической защиты информации «КриптоПро CSP» и «Верба-OW»*
- *Типы электронных подписей.*

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)
Методология оценки безопасности информационных технологий	*							*				
Проектирование подсистем защиты информации от несанкционированного доступа	*							*				
Проектирование подсистем криптографической защиты информации	*							*				
Проектирование подсистем обнаружения компьютерных атак	*							*				
Проектирование защищенных автоматизированных информационных систем	*							*				

Проектирование средств защиты информации от несанкционированного распространения	*							*				

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. Сетевая защита на базе технологий фирмы Cisco Systems. 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.
2. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106 / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков ; науч. ред. Н. А. Гайдамакин ; Урал. гос. техн. ун-т - УПИ .— Екатеринбург : УГТУ-УПИ, 2008. — 182 с.

9.1.2. Дополнительная литература

1. Платонов В. В. Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / В. В. Платонов .— Москва : Академия, 2013 .— 336 с.
2. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах : Учеб. пособие для студентов вузов, обучающихся по спец. "Защищенные телекоммуникационные системы", "Орг. и технология защиты информации", "Комплексное обеспечение информ. безопасности автоматизир. систем" / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. — М. : Радио и связь, 2000 .— 168 с.

9.2. Методические разработки

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 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. Учебно-методический комплекс дисциплины "Основы создания и эксплуатации защищенных компьютерных систем" [Электронный ресурс] / Н. А. Гайдамакин ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (8,17 Мб) .— Екатеринбург : [б. и.], 2007 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1374>.
4. Бакланов В.В. Основы проектирования защищенных телекоммуникационных

систем / Бакланов В.В. — УМК. — 2007. Материалы подготовлены в АИС "Управление учебным процессом". — в корпоративной сети УрФУ. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7115>.

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*	*15*
Домашняя работа №2	*10,1-15*	*15*
Домашняя работа №3	*10,1-15*	*15*
Домашняя работа №4	*10,1-15*	*15*
Домашняя работа №5	*10,1-15*	*15*
Домашняя работа №6	*10,1-15*	*25*

Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий –0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0,4		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Лабораторная работа №1	*10,1-15*	*5*
Лабораторная работа №2	*10,1-15*	*5*
Лабораторная работа №3	*10,1-15*	*5*
Лабораторная работа №4	*10,1-15*	*5*
Лабораторная работа №5	*10,1-15*	*5*
Лабораторная работа №6	*10,1-15*	*5*
Лабораторная работа №7	*10,1-15*	*10*
Лабораторная работа №8	*10,1-15*	*10*
Лабораторная работа №9	*10,1-15*	*10*
Лабораторная работа №10	*10,1-15*	*10*
Лабораторная работа №11	*10,1-15*	*10*
Лабораторная работа №12	*10,1-15*	*10*
Лабораторная работа №13	*10,1-15*	*10*
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	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует

	решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

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

НТК по дисциплине не проводится.

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 для домашних заданий

Домашнее задание №1

1) *При использовании каких криптосхем возникает проблема распространения ключей?*

— асимметричной
— симметричной
— гибридной
— возникает при всех вышеуказанных схемах
— такой проблемы нет.

Обоснуйте свой ответ.

2) *В какой криптосхеме используется принцип «зашифровать может любой, расшифровать — только тот, кто знает секретный ключ»?*

— асимметричной
— симметричной
— ЭЦП
— хэш-
— функции.

Обоснуйте свой ответ.

Домашнее задание №2

1) *Какие из алгоритмов шифрования являются алгоритмами с открытым ключом:*

— DES
— ГОСТ 28147-89
— AES
— RSA.

Обоснуйте свой ответ.

2) *Используются ли указанные средства в любой криптографической системе:*

— криптографические ключи
— разомкнутые линии
— односторонние функции?
Обоснуйте свой ответ.

Домашнее задание №3

1) *Каким образом в симметричной криптосистеме отправитель и получатель используют ключи?*

— один и тот же секретный ключ
— различные секретные ключи
— вообще не используют секретных ключей.
Обоснуйте свой ответ.

2) *Предполагает ли асимметричная криптосистема использование:*

— двух ключей открытого и личного (секретного)
— системы разграничения доступа
— переносных носителей для хранения секретной информации?
Обоснуйте свой ответ.

Домашнее задание №4

1) *Что понимается под системой защиты от несанкционированного использования и копирования:*

— комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов
— комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации
— комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности?
Обоснуйте свой ответ.

2) *Какой из щифров предусматривает три режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки:*

— IDEA
— RSA
— ГОСТ 28147-89
— RC2 или RC4
— DES?
Обоснуйте свой ответ.

Домашнее задание №5

1) *Какая из информаций в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию:*

— электронная подпись
— ключ проверки электронной подписи
— ключ электронной подписи

— сертификат ключа проверки электронной подписи?
Обоснуйте свой ответ.

2) *Какая уникальная последовательность символов, предназначена для создания электронной подписи:*

— квалифицированный сертификат ключа проверки электронной подписи
— ключ проверки электронной подписи
— ключ электронной подписи
— сертификат ключа проверки электронной подписи?
Обоснуйте свой ответ.

Домашнее задание №6

1) *Какой тип имеет электронная подпись, которая должна быть создана с использованием криптографических средств, позволяющая определить автора документа, проверить документ на наличие изменений, не требующая сертификата аккредитованного центра:*

— простая электронная подпись
— усиленная неквалифицированная электронная подпись
— усиленная квалифицированная электронная подпись
— квалифицированный сертификат ключа проверки электронной подписи?
Обоснуйте свой ответ.

2) *К какому классу относятся средства электронной подписи, которые способны противостоять атакам нарушителя как вне пределов, так и в пределах контролируемой зоны:*

— КС1
— КС2
— КС3?
Обоснуйте свой ответ.

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Функциональная схема комплексной системы защиты информации.
2. Применение специализированных программных средств защиты информации, их достоинства и недостатки.
3. Физические носители кодов паролей.
4. Требования к специализированным средствам защиты информации от несанкционированного доступа.
5. Модель управления доступом к защищаемым ресурсам.
6. Общие принципы реализации механизмов разграничения прав доступа.
7. Одноуровневая модель разграничения доступа, достоинства и недостатки.
8. Многоуровневая модель разграничения доступа, достоинства и недостатки.
9. Состав и реализация диспетчера доступа к ресурсам.
10. Алгоритм контроля доступа пользователя к ресурсам защищаемого объекта.
11. Механизмы контроля целостности информации и их реализация
12. Механизмы аудита событий и их реализация

13. Технология доверенной загрузки операционной системы
14. Порядок взаимодействия приложений с криптографическими модулями операционной системы
15. Архитектура системы защищенного документооборота. Структура и функции удостоверяющего центра.
16. Организация виртуальных логических дисков.
17. Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ.
18. Применение специализированных программных средств защиты информации, их достоинства и недостатки.
19. Физические носители кодов паролей.
20. Требования к специализированным средствам защиты информации от несанкционированного доступа.
21. Организация виртуальных логических дисков.
22. Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ.

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

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Средства и методы защиты информации*	**Код модуля** № 1139519
Образовательная программа *Компьютерная безопасность*	**Код ОП 10.05.01/01.02** Учебный план № 5347 (версия 4)
Направление подготовки *Компьютерная безопасность*	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки *специалитет*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

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 В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1.Аннотация содержания дисциплины

Дисциплина реализуется в составе базового модуля *Средства и методы защиты информации* образовательной программы 10.05.01/01.02 Компьютерная безопасность. Содержание дисциплины предусматривает изучение существующих программно-аппаратных средств защиты компьютерной информации и автоматизированных систем в защищенном исполнении, а также изучение подходов и принципов проектирования защищенных автоматизированных информационных систем. В содержание дисциплины входят два основных направления: защита информации к компьютерных сетях и применение специализированных программно-аппаратных средств защиты компьютерной информации.

В ходе изучения дисциплины студенты получают знания о современных средствах криптографической и программно-аппаратной защиты информации. Приобретают навыки, необходимые для практического администрирования защищенных компьютерных систем с применением современных сертифицированных средств защиты информации.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

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

- ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПК-18, способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации;
- ДПК-6, способность обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи.

Знать:

- программно-алгоритмические методы защиты компьютерной информации;
- основные средства и методы защиты компьютерной информации и компьютерных систем;
- основные принципы администрирования защищенных компьютерных систем;
- классификацию и общую характеристику программно-аппаратных средств защиты информации;
- особенности реализации методов защиты информации программно-аппаратными средствами;

Уметь:

– описывать (моделировать) объекты защиты и угрозы безопасности информации;
– применять наиболее эффективные методы и средства программно-аппаратной защиты информации;
– выполнять функции администратора безопасности защищенных компьютерных систем;
– выполнять настройку защитных механизмов программно-аппаратных средств;
– настраивать политику безопасности средствами программно-аппаратных комплексов защиты информации;
– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем;
– организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;
– оценивать и контролировать эффективность мер защиты.

Владеть (демонстрировать навыки и опыт деятельности):
– современными средствами защиты АС от несанкционированного доступа.
– средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа;
– средствами администрирования систем организации виртуальных частных сетей;
– средствами администрирования комплексов криптографической защиты информации.

1.4. Объем дисциплины

Очная форма обучения
УП 5347 (версия 4)

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*9 / 10*
1.	**Аудиторные занятия**	119		68/51
2.	Лекции	51	51	34/17
3.	Практические занятия	68	68	34/34
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	97	17,85	58 / 39
6.	**Промежуточная аттестация**	36	4,66	Э 18/Э 18
7.	**Общий объем по учебному плану, час.**	252	141,51	252
8.	**Общий объем по учебному плану, з.е.**	7		7

Заочная форма обучения не предусмотрена

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	**Технология межсетевого экранирования**	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети

		Интернет с использованием межсетевых экранов. Требования руководящих документов к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.
2	**Организация виртуальных частных сетей**	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet», «Игла», «Верба», «StrongNet». Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
3	**Функции, выполняемые программно-аппаратными средствами защиты компьютерной информации (СЗИ). Применение средств криптографической защиты информации**	Требования к специализированным средствам защиты информации от несанкционированного доступа. Алгоритм работы СЗИ, предназначенного для обработки информации ограниченного доступа. Механизмы организации контроля доступа до загрузки ОС. Взаимодействие СЗИ с BIOS системной платы. Контроль целостности системного программного обеспечения и аппаратных средств. Программно-аппаратная идентификация и аутентификация пользователей. Возможности СЗИ по криптографическому преобразованию информации. Шифрование «по требованию», прозрачное шифрование с организацией виртуальных логических дисков. Способы формирования ключевой информации. Контроль и удаление «технологического мусора». Формирование и поддержка изолированной программной среды. Реализация дискреционной и мандатной моделей разграничения доступа. Обзор современных отечественных средств защиты информации. Основные характеристики системы криптографической защиты информации (СКЗИ) «Верба».

		Инициализация СКЗИ «Верба» на рабочей станции. Генерация, импорт и экспорт ключей. Шифрование и обмен шифрованной информацией. Применение системы криптографической защиты конфиденциальной информации на примере СКЗИ «StrongDisk», «Secret Disk». Основные характеристики СКЗИ. Инициализация системы. Создание и работа с защищенными логическими дисками. Работа с защищенными дисками. Настройка параметров СКЗИ. Управление секретными дисками. Хранение конфиденциальной информации на съемных носителях.
4	**Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение аппаратных модулей доверенной загрузки**	Назначение и возможности СЗИ от НСД, требования, предъявляемые к ним. Использование специализированных аппаратно-программных средств защиты информации от НСД на примере программно-аппаратных комплексов «Страж-NT», «Dallas Lock», «Secret Net». Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Организация учета сменных носителей информации. Регистрация событий. Гарантированное удаление данных. Настройка механизма шифрования данных. Назначение и возможности аппаратных модулей доверенной загрузки на примере комплексов Аккорд-АМДЗ и электронный замок «Соболь». Регистрация пользователей и назначение им персональных идентификаторов и паролей для входа в систему. Управление параметрами процедуры идентификации пользователя. Регистрация событий, имеющих отношение к безопасности системы. Контроль целостности файлов на жестком диске и физических секторов жесткого диска. Защита от несанкционированной загрузки операционной системы со съемных носителей.
5	**Технологии защищенной обработки информации**	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
6	**Обеспечение безопасности АСУ ТП**	Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Уровни АСУ ТП. Уязвимости АСУ ТП.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

Объем модуля (зач.ед.): 19
Объем дисциплины (зач.ед.): 7

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)				Выполнение самостоятельных внеаудиторных работ (колич.)										Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод инояз. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*				
1	Технология межсетевого экранирования	**26**	**16**	6	10		**10**	**10**	**5**	**5**																				
2	Организация виртуальных частных сетей	**43**	**22**	10	12		**21**	**12**	**6**	**6**			**9**	1																
3	Функции, выполняемые программно-аппаратными средствами защиты компьютерной информации (СЗИ). Применение средств криптографической защиты информации	**37**	**16**	8	8		**21**	**12**	**6**	**6**			**9**	1																
4	Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение аппаратных модулей доверенной загрузки	**44**	**32**	14	18		**12**	**12**	**6**	**6**																				
5	Технологии защищенной обработки информации	**41**	**20**	8	12		**21**	**12**	**6**	**6**			**9**	1																
6	Обеспечение безопасности АСУ ТП	**25**	**13**	5	8		**12**	**12**	**6**	**6**																				
	Всего (час), без учета промежуточной аттестации:	**216**	**119**	**51**	**68**		**97**	**70**	**35**	**35**			**27**	**27**																
	Всего по дисциплине (час.):	**252**	**119**				**133**	В т.ч. промежуточная аттестация																			**0**	**36**	**0**	**0**

Зачет

Экзамен

Интегрированный экзамен по модулю

Проект по модулю

*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	Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute	2
1	2	Защита периметра компьютерной сети на базе программно-аппаратных комплексов фирмы Cisco	4
1	3	Межсетевые экраны на базе IP-tables в ОС Linux	4
2	4	Защита сетевого трафика с использованием протокола IPSec в ОС Windows. Организация VPN средствами протокола PPTP	4
2	5	Применение специализированных средств организации VPN на примере «VipNet», «Игла», «Верба», «StrongNet»	8
3	6	Организация защищенного документооборота с использованием криптографических средств, предоставляемых СКЗИ «КриптоПро»	2
3	7	Использование специализированных аппаратно-программных средств защиты информации от несанкционированного доступа. Создание защищенных виртуальных дисков средствами программно-аппаратных комплексов «StrongDisk» и «SecretDisk»	6
4	8	Защита информации от несанкционированного доступа средствами программно-аппаратного комплекса «Dallas Lock»	6
4	9	Реализация многоуровневой политики разграничения доступа средствами программно-аппаратного комплекса «Страж NT»	6
4	10	Комплексная защита информации средствами программно-аппаратного комплекса «Secret NET»	6
5	11	Применение технологии терминального доступа	4
5	12	Построение доменной инфраструктуры на базе AD	8
6	13	Анализ безопасности АСУ ТП	8
		Всего:	**68**

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Система защиты конфиденциальной информации «StrongDisk».*
- *Система защиты корпоративной информации «Secret Disk».*
- *Применение CryptoAPI для работы с СКЗИ КриптоПро CSP*

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)
Технология межсетевого экранирования	*							*				
Организация виртуальных частных сетей	*							*				
Функции, выполняемые программно-аппаратными средствами защиты компьютерной информации (СЗИ). Применение средств криптографической защиты информации	*							*				
Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение аппаратных модулей доверенной загрузки	*							*				
Технологии защищенной обработки информации	*							*				
Обеспечение безопасности АСУ ТП	*							*				

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. Сетевая защита на базе технологий фирмы Cisco Systems. 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.
2. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106 / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков ; науч. ред. Н. А. Гайдамакин ; Урал. гос. техн. ун-т - УПИ. — Екатеринбург : УГТУ-УПИ, 2008. — 182 с.

9.1.2. Дополнительная литература

1. Платонов В. В. Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / В. В. Платонов .— Москва : Академия, 2013 .— 336 с.
2. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах : Учеб. пособие для студентов вузов, обучающихся по спец. "Защищенные телекоммуникационные системы", "Орг. и технология защиты информации", "Комплексное обеспечение информ. безопасности автоматизир. систем" / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. — М. : Радио и связь, 2000 .— 168 с.

9.2. Методические разработки

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 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>.

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
семестр 9

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	*9,1-15*	*30*
Домашняя работа №2	*9,1-15*	*30*
Домашняя работа №3	*9,1-15*	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий –0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практическое занятие №1	*9,1-15*	*15*
Практическое занятие №2	*9,1-15*	*15*
Практическое занятие №3	*9,1-15*	*15*
Практическое занятие №4	*9,1-15*	*15*
Практическое занятие №5	*9,1-15*	*25*
Практическое занятие №6	*9,1-15*	*15*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена*		

Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

семестр 10

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,6**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
	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 –0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практическое занятие №7	*10,1-15*	*15*
Практическое занятие №8	*10,1-15*	*15*
Практическое занятие №9	*10,1-15*	*15*
Практическое занятие №10	*10,1-15*	*15*
Практическое занятие №11	*10,1-15*	*10*
Практическое занятие №12	*10,1-15*	*15*
Практическое занятие №13	*10,1-15*	*15*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

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

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

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

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

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

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

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

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

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач,	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач,

	выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

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

НТК по дисциплине не проводится.

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 для домашних работ

Домашняя работа №1

1) *Можно ли* в*ыяснить открытые сетевые порты с помощью программы*

PING
IPCONFIG
NETSTAT
NET
DIR?
Обоснуйте свой ответ.

2) *Реализуются ли списки контроля доступа в ОС Windows средствами файловой системы:*

FAT16
FAT32
HPFS
NTFS
NWFS?
Обоснуйте свой ответ.

Домашняя работа №2

1) *Реализуется ли защита от утечки конфиденциальной информации в дискреционной модели разграничения доступа:*

средствами файловой системы
правилом NRU
не реализуется?

Обоснуйте свой ответ.

2) *Когда применяется правило «Для каждой четверки субъект-объект-метод-процесс возможность доступа определена однозначно в каждый момент времени»:*

для дискреционной модели разграничения доступа
для мандатной модели разграничения доступа?

Обоснуйте свой ответ.

Домашняя работа №3

1) *Какой аудит событий рекомендуется проводить только на контроллерах домена:*

аудит событий входа в систему
аудит системных событий
аудит отслеживания процессов
аудит доступа к службе каталогов?

Обоснуйте свой ответ.

2) *Каковы функции СЗИ от НСД:*

ограничение на вход в систему
ограничение физического доступа к АИС
контроль целостности ПО, технических средств и данных
доверенная загрузка
реализация политики разграничения доступа
опечатывание системного блока
аудит событий
создание замкнутой программной среды?

Обоснуйте свой ответ.

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

9 семестр

1. Применение специализированных программных средств защиты информации, их достоинства и недостатки.
2. Физические носители кодов паролей.
3. Требования к специализированным средствам защиты информации от несанкционированного доступа.
4. Организация виртуальных логических дисков.
5. Механизмы организации контроля доступа до загрузки ОС. Механизмы доверенной загрузки ОС, реализованные в СЗИ.
6. Подсистемы защиты информации и их реализация в СЗИ от НСД «Страж-NT».
7. Подсистемы защиты информации и их реализация в СЗИ от НСД «Dallas Lock».
8. Подсистемы защиты информации и их реализация в СЗИ от НСД «Secret NET».
9. Организация защищенных вычислительных сетей на базе СЗИ сетевого действия.
10. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
11. Электронные сертификаты. Понятие инфраструктуры открытых ключей.

10 семестр

12. Протоколы и средства организации VPN на сетевом уровне. Назначение, область

применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.

13. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
14. Организация защищенного обмена данными в сети с применением сертифицированных систем.
15. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
16. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
17. Создание защищенных сегментов сетей с использованием межсетевых экранов.
18. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows.
19. Защита рабочих станций с использованием персональных сетевых фильтров.
20. Преимущества технологии терминального доступа. Обеспечение безопасности.
21. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.
22. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

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