МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«Теория и методология информационной безопасности»

Уровень подготовки: высшее образование – подготовка магистров

Направление подготовки магистров
09.04.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Направленность подготовки
Безопасность и защита информации
(наименование программы подготовки)

Квалификация (степень) выпускника
Магистр.

Форма обучения
очная

Уфа 2017

1. Место дисциплины в структуре образовательной программы

Дисциплина «Теория и методология информационной безопасности» является дисциплиной базовой части ОПОП по направлению подготовки 09.04.01 Информатика и вычислительная техника, направленность: Безопасность и защита информации.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от "30" октября 2014 г. № 1420.

Целью освоения дисциплины является формирование у магистров теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач связанных с решением вопросов информационной безопасности, освоение ими типовых приемов решения задач по защите информации, привитие базовых навыков анализа информационной безопасности объекта.

Задачи:

- ознакомление с понятийным аппаратом в области информационной безопасности;
- рассмотрение базовых содержательных положений в области информационной безопасности;
- изучение современной доктрины информационной безопасности РФ;
- определение целей и принципов защиты информации;
- установление факторов, влияющих на защиту информации;
- определение назначения, сущности и структуры систем защиты информации.

Входные компетенции:

На пороговом уровне ряд компетенций был сформирован за счет обучения на предыдущих уровнях высшего образования (специалитет, бакалавриат).

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины, практики, научных исследований, сформировавших данную компетенцию
	способностью анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	**ОПК-6**	пороговый уровень первого этапа освоения компетенции	

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), для которой данная компетенция является входной
	способностью анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитиче-	**ОПК-6**	Базовый уровень	Комплексная система защиты информации на предприятии

	ских обзоров с обоснованными выводами и рекомендациями			
	способностью формировать технические задания и участвовать в разработке аппаратных и (или) программ-мных средств вычислительной техники	**ПК-11**	Базовый уровень	Проектирование защищенных компьютерных систем

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине.

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	способностью анализировать профессиональ-ную информа-цию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитиче-ских обзоров с обоснованными выводами и рекомендациями	**ОПК -6**	- базовый понятийный аппарат в области информационной безопасности; - направления обеспечения безопасности информации; - методики оценки защищенности ин-формационных си-стем.	- определять виды и состав угроз ин-формационной без-опасности; - выбирать и анали-зировать показатели качества и крите-рии оценки систем и отдельных мето-дов и средств защи-ты информации;	- навыками фор-мальной поста-новки и решения задачи обеспече-ния информаци-онной безопасно-сти; - навыками владе-ния методиками определения за-щищенности ин-формационных систем.
	способностью формировать технические за-дания и участво-вать в разработке аппаратных и (или) программ-ных средств вы-числительной техники	**ПК-11**	- современные подходы к построению систем защиты информации; - особенности обеспечения ин-формационной безопасности ком-пьютерных систем.	- определять поли-тику безопасности информационных систем; - пользоваться со-временной научно-технической ин-формацией по ис-следуемым пробле-мам и задачам.	- навыками - использования современных про-граммно-аппаратных средств защиты; - навыками ис-пользования ме-тодов анализа угроз безопасно-сти защищаемой информации.

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часа).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	1 семестр
Лекции (Л)	16

Практические занятия (ПЗ)	30
Лабораторные работы (ЛР)	8
КСР	5
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	85
Подготовка и сдача экзамена	36
Вид итогового контроля (зачет, экзамен)	экзамен

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	**Сущность и понятие информационной безопасности и защиты информации.** Доктрина информационной безопасности РФ. Классификация угроз безопасности. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию. Понятие уязвимости информации. Каналы и методы несанкционированного доступа к информации.	4	6		1	16	27	Р.4.1.1 Р.4.1.2 Р.4.2.2 Р.4.2.3 Р.4.2.4	*лекция-визуализация, проблемное обучение.*
2	**Направления, методы и средства защиты информации.** Виды защиты информации, сферы их действия. Классификация методов защиты информации. Области применения организационных, правовых и инженерно-технических методов защиты информации. Концептуальная модель информационной безопасности.	4	8	4	2	30	48	Р.4.1.1 Р.4.2.1 Р.4.2.2	*лекция-визуализация, проблемное обучение.*
3	**Информационное** воздействие. Воздействующая роль информации. Информационные технологии воздействия. Информационная экология. Средства информационно-технического и информационно-психологического воздействия.	4	8		1	20	33	Р.4.2.1 Р.4.2.2 Р.4.2.5	*лекция-визуализация, проблемное обучение.*
4	**Оценка информационной безопасности предприятия**. Политика безопасности предприятия. Понятие информационного риска. Методики анализа информационных рисков.	4	8	4	1	19	36	Р.4.2.2 Р.4.2.6.	*лекция-визуализация, проблемное обучение.*

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1,2	1	Нормативно-правовая основа информационной безопасности	4
3-6	2	Проблемы обеспечения информационной безопасности	8
7,8	2	Построение модели злоумышленника	4
9,10	2	Угрозы современных информационных технологий	4
11-13	3	Информационные технологии воздействия	6
14,15	4	Политика безопасности предприятия	4

Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Стеганографические способы защиты информации	4
2	4	Оценка информационных рисков. FCMBuilder	4

4. Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1.Основная литература

1. Грибунин, В. Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов / В. Г. Грибунин, В. В. Чудовский. – М. : Академия, 2009. – 411 с.
2. Семененко, В. **А.** Информационная безопасность : / В. А. Семененко ; МГИУ, Институт дистанционного образования .— 3-е изд., стер. – Москва : МГИУ, 2008 . – 277 с.

4.2. Дополнительная литература

1. Семкин, С. Н. Основы правового обеспечения защиты информации : учебное пособие для вузов/ С. Н. Семкин, А. Н. Семкин . – М.: Горячая линия-Телеком, 2007. – 238 с.
2. Малюк, А. А. Информационная безопасность : концептуальные и методологические основы защиты информации : учебное пособие для студентов вузов / А. А. Малюк . – М. : Горячая линия-Телеком, 2004 . – 280 с.
3. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации». http://base.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=183056&fld=134&from=165971-0&rnd=208987.08123980324582192&
4. Доктрина информационной безопасности РФ. (утв. Президентом РФ 09.09.2000 N Пр-1895) http://base.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=28679&rnd=208987.49975524732130117&SEARCHPLUS=%C4%EE%EA%F2%F0%E8%ED%E0%20%C8%C1%20%D0%D4&EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO&SRD=true&SRDSMODE=QSP_GENE RAL.
5. **Лукьянович, А. В**. Информационное воздействие СМИ на безопасность населения / А. В. Лукьянович, М. В. Омельченко, Т. И. Афлятунов // Безопасность жизнедеятельности . – 2015. – № 9 .– С. 37-43.
6. **Атаманов, Г. А.** Азбука безопасности. Информационные вызовы, риски и угрозы / Г. А. Атаманов // Защита информации. Инсайд . – 2014 . – № 1 . – С. 6-12 .

5. Материально-техническое обеспечение дисциплины

1. Учебная аудитория, оснащенная мультимедийным проектором – 5-301, 5-314.

2. Дисплейный класс с использованием IBM-совместимых персональных компьютеров под управлением ОС Windows, объединенных в локальную сеть с выходом в глобальную сеть Internet, оснащенных антивирусными средствами (AVP Касперского, ESET NOD32 Anti-virus и др.), архиваторами WinZip и WinRar – 5-304.