МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

Уровень подготовки: высшее образование – подготовка кадров высшей квалификации

Направление подготовки научно-педагогических кадров высшей квалификации
(магистратура)
27.04.03 Системный анализ и управление
(код и наименование направления подготовки, специальности)

Направленность подготовки
Теория и математические методы системного анализа и управления в технических системах
(наименование профиля подготовки, специализации)

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Уфа 2016

Исполнители:

должность	подпись	расшифровка подписи

Заведующий кафедрой

наименование кафедры	*личная подпись*	*расшифровка подписи*

Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность и защита информации» является дисциплиной базовой части.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки научно-педагогических кадров высшей квалификации (магистратура) *27.04.03 «Системный анализ и управление»,* утвержденного приказом Министерства образования и науки Российской Федерации от "30" июля 2014 г. № 874 и приказом Министерства образования и науки Российской Федерации от 30.04.2015 N 464 "О внесении изменений в федеральные государственные образовательные стандарты высшего образования (уровень подготовки кадров высшей квалификации)".

Целью освоения дисциплины является изучение магистрантами понятийного аппарата информационного взаимодействия в сложных организационно-технических системах, теоретических основ и методической базы построения защищенных информационных систем (ИС) как инструмента управления в различных сферах деятельности, а также основ управления информационной безопасностью (ИБ) в ИС.

Задачи:

1. Сформировать знания об основных аспектах управления информационной безопасностью;
2. Изучить принципы и особенности реализации основных функций управления: планирования, контроля, принятия решений и прогнозирования;
3. Сформировать представления магистрантов о современных подходах к построению систем управления информационной безопасностью;
4. Рассмотреть конкретные примеры решения задач в области планирования защиты информации и оперативного управления информационной безопасностью.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), сформировавшего данную компетенцию
1	Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	ОК-2	пороговый и базовые уровни	Дисциплина: Информационная безопасность и защита информации
2	Способность разрабатывать новые методы и адаптировать существующие методы системного анализа вариантов эффективного управления техническими объектами	ПК-2	пороговый и базовые уровни	Дисциплина: Информационная безопасность и защита информации

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), для которой данная компетенция является входной

Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	ОК-2	•фундаментальные понятия информационного взаимодействия; •архитектуру безопасности современных информационных систем, основы ее построения; •методы поддержки принятия решений, стратегии выбора основных сервисов безопасности.	•разрабатывать базовую структуру сети согласно бизнес-процессам по требованиям обеспечения производительности, доступности и безопасности •формулировать и решать проблемы выбора мер противодействия и средств защиты, применяя научные подходы; •работать в коллективе, занимающимся проектированием и эксплуатацией систем обеспечения информационной безопасности; •проводить моделирование объекта защиты и системы принятия решений в области информационной безопасности.	•навыками реализации мероприятий по защите информации в современных информационных системах на основе разработки алгоритмического и программного обеспечения для автоматизированного принятия решений.
2	Способность разрабатывать новые методы и адаптировать существующие методы системного анализа вариантов эффективного управления техническими объектами	ПК-2	•модель процесса планирования рационального модульного состава системы обеспечения информационной безопасности; •современные программные продукты управления информационной безопасностью.	•применять принципы решения управленческих задач, связанных с проблемами выбора, размещения, распределения и др.; •применять навыки и теоретические подходы при решении задач построения систем обеспечения	•применением методов принятия решений для обоснованного выбора средств защиты.

				информационной безопасности, а так же и управления безопасностью.	

Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	1 семестр
Лекции (Л)	14
Практические занятия (ПЗ)	4
Лабораторные работы (ЛР)	16
КСР	4
Курсовая проект работа (КР)	не предусмотрено планом
Расчетно - графическая работа (РГР)	не предусмотрено планом
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.)	97
Подготовка и сдача экзамена	
Подготовка и сдача зачета	1
Вид итогового контроля (зачет, экзамен)	Зачет

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	**Введение.** Анализ существующих стандартов и основных аспектов управления защитой информации. Обзор современных систем управления защитой информации и средств автоматизации управления рисками нарушения информационной безопасности. **Состав и основы функционирования ИС как объекта защиты.** Системотехнические основы построения сложных систем. Организационные процессы как объект управления. Особенности организационно-технических система управления. ИС как инструмент управления бизнесом, финансовой, банковской деятельностью, современным производством. Современная информационная система, состоящая из двух крупных блоков: информационной инфраструктуры и информационных сервисов. Телекоммуникационная система (ТКС) как совокупность средств обработки информационных ресурсов и среда, обеспечивающая потребление информационных услуг. Определение ТКС. Основы ее построения. Задачи защиты информации в ТКС.	3				17	20	Р 6.1 №1 Р 6.1 №2	При проведении лекционных занятий: – лекция классическая; проблемная лекция; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
2	**Декомпозиция проблемы разрешения противоречий в области защиты информации на основе системного анализа.** Разработка архитектуры и функциональной модели системы управления защитой информации в сегменте корпоративной	4	2		2	20	28	Р 6.1 №1 Р 6.1 №3 Р 6.2 №1 Р 6.2 №2	При проведении лекционных занятий: – лекция классическая; проблемная

	информационной системы. Разработка модели объекта защиты – сегмента корпоративной информационной системы. Формирование концепции построения модели угроз информационной среде сегмента корпоративной информационной системы.								лекция; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
3	**Основы обеспечения информационной безопасности в инфраструктуре ИС.** 2.1Требования пользователей к информационной инфраструктуре: производительность, доступность, безопасность. Пример сетевой конфигурации с высоким уровнем доступности. Разбиение ТКС на внешние и внутренние подсети. Необходимость защиты периметра и размещения внешних серверов (почтовый, web и другие) в отдельных экранированных сегментах. Меры обеспечения безопасности удаленного доступа через общедоступные сети. Обеспечение безопасности стратегически важных сегментов во внутренней подсети. Средства обеспечения безопасности особо важных внутренних ресурсов. 2.2 Стратегия выбора основных сервисов безопасности в ИС (на примере МСЭ и IDS). Межсетевые экраны как важный элемент архитектуры безопасности. Преимущества МСЭ. Недостатки МСЭ. Технологии межсетевого экранирования. Типы IDS т модели обнаружения. Узловые IDS (HIDS). Сетевые IDS (NIDS). Модель	4	1		2	30	37	Р 6.1 №1	При проведении лекционных занятий: – лекция классическая; проблемная лекция; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.

	обнаружения признаков (сигнатур). Модель обнаружения аномалий. Преимущества и недостатки.								
4	**Интеллектуальная поддержка управления информационной безопасности в ИС** Методологические основы управления защитой информации в инфраструктуре информационной системы. Разработка принципов интеллектуальной поддержки оперативного управления защитой информации в информационной системе. Формализованное описание метода принятия решений, адаптированного для выбора рационального варианта реагирования на события безопасности. Разработка моделей противодействия угрозам информационной безопасности в условиях неопределенности для типовых путей распространения атак в сегменте корпоративной информационной системы. Принципы интеллектуальной поддержки организационно- технического управления защитой информации в инфраструктуре информационной системы. Разработка модели процесса планирования рационального модульного состава системы защиты информации. Формализованное описание процесса планирования рационального модульного состава СЗИ. Интеллектуальная поддержка принятия решений в контуре организационно-технического управления защитой информации. Модели прогнозирования уровня защищенности информации в инфраструктуре информационной системы и метод оценки риска.	3	1	16		30	50	Р 6.1 №1 Р 6.1 №3 Р 6.2 №1 Р 6.2 №2	При проведении лекционных занятий: – лекция классическая; проблемная лекция; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.

Занятия, проводимые в интерактивной форме, составляют 30 % от общего количества аудиторных часов по дисциплине «Информационная безопасность и защита информации».

Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	3	Комбинаторно-морфологический метод синтеза рациональных наборов средств защиты для систем защиты информации: Выбор рационального состава средств защиты периметра для системы обеспечения информационной безопасности.	4
2	3	Метод выбора рационального варианта реагирования на события нарушения информационной безопасности.	4
3	3	Разработка политики безопасности на основе математической модели ролевого разграничения доступа.	4
4	3	Метод линейной свертки и метод ранжирования альтернатив для поддержки принятия решения по выбору средств защиты.	4

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Анализ нормативно методических документов Гостехкомиссии России, Положение ФСБ России, методических документов и приказов ФСТЭК.	1
2	2	Анализ ГОСТ ISO/IEC и ИСО МЭК. ГОСТ по управлению информационной безопасностью.	1
3	3	Методы и средства анализа рисков нарушения информационной безопасности.	2

Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература

1. Управление защитой информации на основе интеллектуальных технологий / М.Б. Гузаиров, И.В. Машкина — М.: Машиностроение, 2013. — 241 с. ISBN.

2. Основы управления информационной безопасностью / А.П. Курило, Н.Г. Милославская, А.И. Толстой, М.Ю. Сенаторов. - М.: Горячая линия-Телеком, 2012. - 244 с.

3. Машкина, И.В. Анализ риска объекта информатизации: учебное пособие / И.В. Машкина, Е.С. Степанова, Т.О. Вишнякова, Уфимск. гос. авиац. техн. ун-т. – Уфа: УГАТУ, 2011. – 112 с.

Дополнительная литература

1. Управление рисками информационной безопасности / Н.Г. Милославская, А.И. Толстой, М.Ю. Сенаторов. - М.: Горячая линия-Телеком, 2014. — 130 с.

2. Управление инцидентами ИБ и непрерывностью бизнеса / Н.Г. Милославская, А.И. Толстой, М.Ю. Сенаторов. - М.: Горячая линия – Телеком, 2012 – 170 с.

Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки УГАТУ http://www.library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Образовательные технологии

№	Наименование	Доступ, количество одновременных пользователей	Реквизиты договоров с правообладателями
Ресурса			
1	СПС «КонсультантПлюс»	По сети УГАТУ, без ограничения	Договор 1392/0403-14 от 10.12.14
2	СПС «Гарант»	По сети УГАТУ, без ограничения	ООО «Гарант-Регион, договор 291/-0107-14, от25.04.14
Программного продукта			
1	Kaspersky Endpoint Security для бизнеса	500 компьютеров	Лицензия 13C8-140128-132040
2	Программный комплекс – операционная система Microsoft Windows	1800 компьютеров, на которые распространяется право пользования	№ договора ЭФ-193/0503-14
3	Программный комплекс – Microsoft Office	1800 компьютеров, на которые распространяется право пользования	№ договора ЭФ-193/0503-14

Материально-техническое обеспечение дисциплины

Для проведения лабораторных работ используются компьютерные классы кафедры вычислительной техники и защиты информации, оборудованные современной вычислительной техникой, из расчета не менее одного рабочего места на двух обучающихся при проведении занятий в данных классах.

При выполнении лабораторных работ используются персональные компьютеры.

Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЗАКЛЮЧЕНИЕ

Научно-методического совета

по УГСН 27.00.00 Управление в технических системах

Настоящим подтверждаю, что представленный комплект аннотаций рабочих программ учебных дисциплин по направлению подготовки магистра 27.04.03 Системный анализ и управление, реализуемой по очной форме обучения, соответствует рабочим программам учебных дисциплин указанной выше образовательной программы.

Председатель НМС _____ В.Е.Гвоздев