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

«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Уровень подготовки: высшее образование – магистратура

Направление подготовки
10.04.01 Информационная безопасность
(код и наименование направления подготовки)

Направленность подготовки
Информационная безопасность
(наименование программы подготовки)

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Разработана в соответствии

с ФГОС ВПО, Приказ МОиН РФ от 28.10.2009, № 497

Актуализирована в соответствии

с ФГОС ВО, Приказ МОиН РФ от 01.12.2016, № 1513

Уфа 2016

Исполнитель:
профессор _____ И.А.Машкина
должность *личная подпись* *расшифровка подписи*

Заведующий кафедрой
ВТиЗИ _____ В.И.Васильев
наименование кафедры *личная подпись* *расшифровка подписи*

1. Место дисциплины в структуре образовательной программы

Дисциплина «Управления информационной безопасностью» является дисциплиной базовой части.

Рабочая программа составлена в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090900 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 497;

Рабочая программа актуализирована в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1513.

Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

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), практики, научных исследований, сформировавших данную компетенцию
1	способность анализировать направления развития (телекоммуникационных)	ПК-1	пороговый и базовые уровни	Сформирована на этапе бакалаврской подготовки

	технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты			
2	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ПК-14	пороговый и базовые уровни	Сформирована на этапе бакалаврской подготовки

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	способность анализировать направления развития (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ПК-1	Повышенный уровень	Государственная итоговая аттестация

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	способность анализировать направления развития (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать	ПК-1	•фундаментальные понятия информационного взаимодействия; •архитектуру безопасности современных информационных систем, основы ее построения; •методы	•разрабатывать базовую структуру сети согласно бизнес-процессам по требованиям обеспечения производительности, доступности и безопасности •формулировать и решать проблемы	•навыками реализации мероприятий по защите информации в современных информационных системах на основе разработки алгоритмического и программного

	затраты и риски, формировать политику безопасности объектов защиты		поддержки принятия решений, стратегии выбора основных сервисов безопасности.	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.	обеспечения для автоматизированн ого принятия решений.
2	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационно й безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ПК-14	•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 информационной безопасности, а так же и управления безопасностью.	•применением методов принятия решений для обоснованного выбора средств защиты.

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72часа).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	1семестр 72 часа/2 ЗЕ
Лекции (Л)	6
Практические занятия (ПЗ)	6
Лабораторные работы (ЛР)	12
КСР	2

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.)	37
Подготовка и сдача экзамена	
Подготовка и сдача зачета	9
Вид итогового контроля (зачет, экзамен)	Зачет

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая магистрантам	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.	2	1			7	10	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	**Основы обеспечения информационной безопасности в инфраструктуре ИС.** 2.1Требования пользователей к информационной инфраструктуре: производительность, доступность, безопасность.	2	1		2	10	15	Р 6.1 №1	При проведении лекционных занятий: – лекция классическая; проблемная

	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 и модели обнаружения. Узловые IDS (HIDS). Сетевые IDS (NIDS). Модель обнаружения признаков (сигнатур). Модель обнаружения аномалий. Преимущества и недостатки.								лекция; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
3	**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	2	4	12		20	38	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;

	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.								– обучение на основе опыта.

Занятия, проводимые в интерактивной форме, составляют 23% от общего количества аудиторных часов по дисциплине «Управление информационной безопасностью».

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

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.	2
2	2	Анализ ГОСТ ISO/IEC и ИСО МЭК. ГОСТ по управлению информационной безопасностью.	2
3	3	Методы и средства анализа рисков нарушения информационной безопасности.	2

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

6.1 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.[URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5178]

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.

6.2Дополнительная литература

1. Управление инцидентами ИБ и непрерывностью бизнеса / Н.Г. Милославская, А.И. Толстой, М.Ю. Сенаторов. - М.: Горячая линия – Телеком, 2014 – 170 с.

6.3. 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.

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
1.	ЭБС «Лань» http://e.lanbook.com/	41716	С любого компьютера, имеющего выход в Интернет, после регистрации в ЭБС по сети УГАТУ	Договор № ЕД – 1185/0208-16 от 08.08.2016
2.	ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru	1225	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Учредительный договор Ассоциации образовательных организаций «Электронное образование Республики Башкортостан» от 29.11.2013
3.	Консорциум аэрокосмических вузов России http://elsau.ru/	1235	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Договор о сетевом взаимодействии от 15.12.2014
4.	Электронная коллекция образовательных ресурсов УГАТУhttp://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus	528	С любого компьютера по сети УГАТУ	Свидетельство о регистрац. №2012620618 от 22.06.2012

5.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №2255/0208-15 от 23.12.2015
6.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и дипломных работ	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России) Сублиц. договор №ProQuest/15152/0208-16 от 02.06.2016
7.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор 3К-2318/0106-15 от 30.12.2015
8.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208-16 от 15.03.2016
9.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии-1место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
10.	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9919 полнотекстовых журналов	С любого компьютера, имеющего выход в Интернет, после регистрации в НЭБ на площадке	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006

			библиотеки УГАТУ	
11.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор№Questel/15146/0208-16 от 02.06.2016
12.	Научные полнотекстовые журналы издательства Taylor& Francis Group* http://www.tandfonline.com/	1700 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №T&F/151 44/0208-16 от 02.06.2016
13.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. жрнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
14.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и

				науки РФ и ГПНТБ России Сублиц. договор №OUP-151 43/0208-16 от 02.06.2016
15.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наим. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016
16.	Научный полнотекстовый журнал Science The American Association for the Advancement of Science http://www.sciencemag.org	1 наимен. журнала.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151 45/0208-16 от 02.06.2016
17.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016
18.	Научные полнотекстовые ресурсы Optical Society of America* http://www.opticsinfobase.org	19 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в	В рамках Государственного контракта от 17.02.2016 г.

	/		Интернет	№14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
19.	База данных GreenFile компании EBSCO* http://www.greeninfoonline.com	5800 библиографич записей, частично с полными текстами	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)
20.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич записей		В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
21.	Архив научных полнотекстовых журналов зарубежных издательств*- http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849– 1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996)	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

	Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)			

* Периодические издания получены по Гранту и на баланс библиотеки не принимались.

7. Образовательные технологии

При реализации дисциплины *«Управление информационной безопасностью»* применяются классические образовательные технологии. Формы работы студентов: лекционные занятия, практические и лабораторные занятия, написание рефератов, выполнение контрольных работ (преимущественно в тестовой форме), решение кейс-задач во время лабораторных работ. В процессе проведения практических занятий рекомендуется использовать интерактивные формы проблемного обучения.

Дисциплина «*Управление информационной безопасностью*» разбита на контролируемые разделы, комплексы знаний и умений в составе которых, подлежат контролю.

Контроль включает в себя выполнение письменных контрольных работ, преимущественно в тестовой форме, защиты лабораторных работ и представление рефератов.

Подбор вопросов для очередного тестирования (контрольной работы) осуществляется на основе изученного теоретического материала.

В качестве основной формы контролируемой самостоятельной работы студента рекомендуется использовать написание рефератов по выбранной заранее тематике. При написании реферата студент должен в соответствии с требованиями к оформлению работ сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

Для успешной подготовки к итоговому контролю в форме зачета необходимо выполнить следующие контрольные мероприятия:

1. Выполнить тестовые задания по материалам каждого раздела учебного курса.
2. Выполнить все лабораторные работы по дисциплине с последующей защитой. Защита лабораторных работ требует заполнения отчетов, которые составляются в электронном (или печатном) виде. Файлы отчетов с материалами выполненных заданий лабораторных работ должны быть представлены преподавателю. В отчетах должна быть представлена следующая информация: тема работы; цель работы; общая постановка задачи; результаты выполнения работы с программными фрагментами и скриншотами; ответы на контрольные вопросы.
3. Представить реферат и ответить на контрольные вопросы преподавателя по его теме.

Зачет при успешном выполнении указанных пунктов (пп. 1, 2, 3) проставляется без дополнительного опроса. При наличии существенных недостатков в их выполнении проводится дополнительный опрос по 2-3 пунктам перечня вопросов из фонда оценочных средств по различным разделам курса в устной или письменной форме.

9 . 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.

Лекционные ауд. 5-301, 5-314. Персональный компьютер (1 шт), мультимедийный проектор (1шт.) Программный комплекс – операционная система Microsoft Windows № договора ЭА-269/0503-16 , 1800 компьютеров. Программный комплекс – Microsoft Office № договора ЭА-269/0503-16 , 1800 компьютеров.

Ауд. 5-304 Компьютерный класс №1, персональный компьютер (6 шт), коммутатор (1шт.) Программный комплекс – операционная система Microsoft Windows № договора ЭА-269/0503-16 , 1800 компьютеров.

Программный комплекс – Microsoft Office № договора ЭА-269/0503-16 , 1800 компьютеров.

Ауд. 5-221 Кабинет для самостоятельной работы студентов персональный компьютер (2 шт) Программный комплекс – операционная система Microsoft Windows № договора ЭА-269/0503-16 , 1800 компьютеров.

Программный комплекс – Microsoft Office № договора ЭА-269/0503-16 , 1800 компьютеров.

10. 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.