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 – бакалавриат

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

Направленность подготовки (профиль)
Безопасность автоматизированных систем
(наименование профиля подготовки)

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Год начала подготовки – 2015

Уфа 2016

Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» является обязательной дисциплиной базовой части.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 28 октября 2009 г. № 496, а также в соответствии с Приказом Министерства образования и науки Российской Федерации от 19 декабря 2013 г. N 1367 г. «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» и актуализирована в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 01 декабря 2016 г. № 1515. Является неотъемлемой частью основной профессиональной образовательной программы (ОПОП).

Цели освоения дисциплины – изучение студентами понятийного аппарата информационного взаимодействия в сложных организационно-технических системах, теоретических основ и методической базы построения информационных систем (ИС) как инструмента управления в различных сферах деятельности, а также основ обеспечения информационной безопасности ИС.

Задачи:

1. Сформировать у обучаемых представления и основные теоретические положения об общих принципах построения сложных систем, о структуре и функционировании ИС;
2. Сформировать у обучаемых знания о концептуальных основах обеспечения информационной безопасности в ИС;
3. Сформировать у обучаемых знания об основных аспектах управления информационной безопасностью в ИС;
4. Сформировать у обучаемых знания методов принятия решений для обоснованного выбора средств защиты в ИС;
5. Приобрести обучаемыми умения и практические навыки защиты информации в современных информационных системах на основе разработки алгоритмического и программного обеспечения для автоматизированного принятия решений.

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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОК-7	- основные аспекты управления защитой информации	- проводить анализ уровня защищенности информации	- навыками применения методов принятия решений для обоснованного выбора средств защиты
2	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ОПК-4	- современные системы управления информационной безопасность ИС	- разрабатывать базовую структуру сети согласно бизнес-процессам и требованиям архитектуры безопасности	- навыками применения методов принятия решений для обоснованного выбора средств защиты

3	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13	- принципы интеллектуальной поддержки принятия решений по планированию и оперативному управлению информационной безопасностью ИС	- применять принципы решения управленческих задач, связанных с проблемами выбора, размещения, планирования	- навыками проведения мероприятий по защите информации в современных информационных системах на основе разработки алгоритмического обеспечения для автоматизированного принятия решений

Содержание разделов дисциплины

№	Наименование и содержание разделов
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.
2	**Состав и основы функционирования ИС как объекта защиты** Классификация ИСБ. Принципы организации ИСБ. Структурные схемы ИСБ. Существующие ИСБ. 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. Взаимодействие ТКС с прикладными программными системами. Угрозы безопасности информации в ИС. Задачи защиты информации в ТКС и четыре подхода к разработке технологий защиты. Анализ схем информационного взаимодействия в ТКС с коммутацией пакетов с точки зрения ИБ.
3	**Основы обеспечения информационной безопасности в инфраструктуре ИС** Требования пользователей к информационной инфраструктуре: производительность, доступность, безопасность. Требования к скорости передачи данных. Обеспечение избыточности и отказоустойчивости путем исключения из сетевой архитектуры единых точек сбоя. Дополнительные методы обеспечения отказоустойчивости. 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. Вопросы безопасности, связанные с коммуникационным оборудованием. Сетевое оборудование и вопросы обеспечения безопасности. Коммутаторы, маршрутизаторы. Методы обеспечения безопасности, реализуемые при использовании коммутаторов. 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. Пакетные фильтры, их стратегии реализации. Преимущества пакетных фильтров, их недостатки. Шлюзы сеансового уровня, шлюзы приложений. Основное преимущество, недостатки. МСЭ с адаптивной проверкой пакетов, механизм их действия, преимущества и недостатки. Комплексные МСЭ. Дополнительные функции МСЭ. IDS первого поколения. Системы IDS второго поколения. Типы IDS, модели обнаружения. Узловые IDS (HIDS). Сетевые IDS (NIDS). Модель обнаружения признаков (сигнатур). Правила обнаружения сигнатур. Преимущества и недостатки IDS с обнаружением признаков. Модель обнаружения аномалий. Перечень отслеживаемых событий. Недостатки ADS. Системы предотвращения вторжений IPS. Последствия использования IPS. Необходимость повышения точности обнаружения.

№	Наименование и содержание разделов
	Три компонента безопасности: оборона, обнаружение, сдерживание. Политика безопасности ИС, политика разграничения доступа.
4	**Интеллектуальная поддержка управления информационной безопасности в ИС** Методологические основы управления защитой информации в инфраструктуре информационной системы. Принятие решений в системах управления информационной безопасностью. Принципы интеллектуальной поддержки оперативного управления защитой информации в инфраструктуре информационной системы. Принципы интеллектуальной поддержки организационно- технического управления защитой информации в информационной системе.

Подробное содержание дисциплины, структура учебных занятий, трудоемкость изучения дисциплины, входные и исходящие компетенции, уровень освоения, определяемый этапом формирования компетенций, учебно-методическое, информационное, материально-техническое обеспечение учебного процесса изложены в рабочей программе дисциплины.