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 – специалитет

Специальность
10.05.05 «Безопасность информационных технологий
в правоохранительной сфере»
(код и наименование специальности)

Специализация
Технологии защиты информации в правоохранительной сфере
(наименование специализации)

Квалификация (степень) выпускника
Специалист

Форма обучения
очная

Год начала подготовки – 2013

Уфа 2017

Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» является дисциплиной базовой части основной профессиональной образовательной программы (ОПОП).

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по специальности 090915 Безопасность информационных технологий в правоохранительной сфере, утвержденного приказом Министерства образования и науки Российской Федерации от "01" февраля 2011 г. № 132, 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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, утвержденного приказом Министерства образования и науки Российской Федерации 19 декабря 2016 г. № 1612. Является неотъемлемой частью основной профессиональной образовательной программы.

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 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 студентов 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.

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 принимать организационно-управленческие решения	ОК-8	фундаментальные понятия информационного взаимодействия	проводить анализ уровня защищенности информации	навыками применения методов принятия решений для обоснованного выбора средств защиты
2	Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ПК-1	архитектуру безопасности современных информационных систем, основы ее построения	разрабатывать базовую структуру сети согласно бизнес-процессам и требованиям архитектуры безопасности	навыками применения методов принятия решений для обоснованного выбора средств защиты
3	Способность организовывать и проводить мероприятия по контролю за	ПК-3	принципы интеллектуальной поддержки принятия решений	формулировать и решать проблемы выбора мер противодействия и	навыками проведения мероприятий по защите информации

	обеспечением защиты информации, проводить анализ эффективности системы защиты информации		по планированию и оперативному управлению информационной безопасностью ИС	средств защиты, применяя научные подходы	в современных информационных системах на основе разработки алгоритмического обеспечения для автоматизированног о принятия решений
4	Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации	ПК-18	современные программные продукты управления информационной безопасностью	работать в коллективе, занимающимся проектированием и эксплуатацией систем обеспечения информационной безопасности	Навыками проведения мероприятий по защите информации в современных информационных системах на основе разработки программного обеспечения для автоматизированного принятия решений
5	Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации	ПК-28	методы обеспечения безопасности, связанные с коммуникационн ым оборудованием	применять навыки и теоретические подходы при решении задач построения систем обеспечения информационной безопасности, а также и управления безопасностью	навыками по разработке моделей разграничения доступа к информации в ИС

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

№	Наименование и содержание разделов
	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. 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.