МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра автоматизированных систем управления

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки (специальность)
09.03.03 Прикладная информатика

Направленность подготовки (профиль)
Прикладная информатика в экономике

Квалификация выпускника
бакалавр

Форма обучения
очная

УФА — 2015

Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» является дисциплиной базовой части.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки / специальности 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от "12" марта 2015 г. № 207.

Целью освоения дисциплины является: раскрытие сущности и значения информационной безопасности, определение ее места в системе национальной безопасности, определение основных положений информационной безопасности.

Задачи:

- Сформировать знания по правилам описания административных регламентов и электронных административных регламентов
- Знание понятийного аппарата в области информационной безопасности
- Сформировать знания по базовым содержательным положениям в области инфор¬мационной безопасности
- Знание современной доктрины информационной безопасности, целей и принципов защиты информации, факторов, влияющих на защиту информации, структуры угроз защищаемой информации
- Сформировать знания по правилам определения сущности компонентов защиты информации

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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-4	виды информационно-коммуникационных технологий, используемые для решения профессиональных задач	—	—
2	способностью принимать участие в организа-	ПК-18	виды и состав угроз информационной безопасности; мо-	классифицировать защищаемую информацию по ее соб-	навыками анализа безопасности информационных си-

	ции ИТ-инфраструктуры и управлении информационной безопасностью		дели безопасности и их применение	ственникам, видам тайн и материальным носителям	стем

Содержание разделов дисциплины

№	Наименование и содержание раздела
1	Информационная безопасность и уровни ее обеспечения: Тема 1. Понятие "информационная безопасность". Тема 2. Составляющие информационной безопасности. Система формирования режима информационной безопасности.
2	Уровни формирования режима информационной безопасности: Тема 1. Угрозы безопасности информации и их классификация. Тема 2. Структура угроз защищаемой информации. Классы угроз информационной безопасности. Критерии безопасности компьютерных систем – "Оранжевая книга".
3	Абстрактные модели защиты информации. Модель элементарной защиты: Модель Гогена-Мезигера. Сазерлендская модель защиты. Модель защиты Кларка-Вильсона.
4	Каналы и методы несанкционированного доступа к информации. : Каналы несанкционированного доступа к информации. Выявление каналов доступа к информации. Деловая разведка как канал получения информации. Модель потенциального нарушителя.
5	Источники, способы и результаты дестабилизирующего воздействия на информацию: Тема 1. Классификация угроз информационной безопасности. Угрозы секретности и целостности. Тема 2. Классификация уязвимостей безопасности. Определение источников дестабилизирующего воздействия на информацию. Тема 3. Методика выявления способов воздействия на информацию. Определение причин и условий дестабилизирующего воздействия на информацию.
6	Классификация уязвимостей безопасности: Определение источников дестабилизирующего воздействия на информацию. Методика выявления способов воздействия на информацию. Определение причин и условий дестабилизирующего воздействия на информацию.
7	Информационная безопасность вычислительных сетей: Тема 1. Особенности информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. Тема 2. Механизмы обеспечения "информационной безопасности". Криптография и шифрование.
8	Информационный риск. Стратегия управления риском: Сущность понятия «риск». Понятие информационного риска. Управление информационными рисками.
9	Компьютерные вирусы и защита от них: Тема 1. Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Тема 2. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ.
10	Модели защиты информации и определение политики безопасности: Тема 1. Дискреционная модель Харрисона-Руззо-Ульмана. Классическая мандатная модель политики безопасности Белла-Лападулы. Ролевая модель управления доступом. Тема 2. Определение

	политики безопасности. Концептуальные основы для построения защиты информации от несанкционированного доступа в вычислительной системе.
11	Методы обеспечения информационной безопасности Российской Федерации: Тема 1. Правовой статус информации. Концепция обеспечения доступа граждан к информации государства. Регулирование доступа граждан к информации государства. Безопасность инфраструктуры раскрытия информации государства. Тема 2. Государственная тайна. Сведения, отнесенные к гостайне. Степени секретности гостайны.

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.

ЗАКЛЮЧЕНИЕ

Научно-методического совета

по направлению подготовки (специальности)
09.03.03 Прикладная информатика

Настоящим подтверждаю, что представленный комплект аннотаций рабочих программ учебных дисциплин по направлению подготовки (специальности)
09.03.03 Прикладная информатика
по профилю (направленности) Прикладная информатика в экономике,
реализуемой по форме обучения очной, заочной
соответствует рабочим программам учебных дисциплин указанной выше образовательной программы.

Председатель НМС  А.И. Фрид
личная подпись

30.06.2015
дата