МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский государственный авиационный технический университет»

Кафедра Информатики

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«Методы и средства предотвращения внештатных ситуаций в организационно-технических системах»

Специальность
27.05.01 Специальные организационно-технические системы
(код и наименование направления подготовки)

Специализация № 2
Информационно-аналитическая деятельность в специальных организационно-технических системах
(наименование специализации)

Квалификация (степень) выпускника
Специалист

Форма обучения
Очная

Уфа 2016

1 Место дисциплины в структуре ОПОП ВО

Предшествующими дисциплинами, на которых непосредственно базируется дисциплина «Методы и средства предотвращения внештатных ситуаций в организационно-технических системах» являются:

- Информатика;
- Вычислительные машины, системы и сети;
- Дисциплина по выбору 1 ГСЭ (Правовая и информационная поддержка организационно-технических систем, Международное право в организационно-технических системах);
- Дисциплина по выбору 8 ПЦ (Операционные системы и среды, Системное администрирование).

Вместе с тем дисциплина «Методы и средства предотвращения внештатных ситуаций в организационно-технических системах» является основополагающей для изучения дисциплин:

- Интернет-технологии.

Цели и задачи освоения дисциплины

Цель освоения дисциплины – овладение студентами основными понятиями, методами и средствами предотвращения внештатных ситуаций в организационно-технических системах; приобретение студентами навыков и умений по построению систем искусственного интеллекта для поддержки принятия решений в организационно-технических системах.

Задачи:

1. Образовательная – в соответствии с ГОС сообщать студентам системные знания о наиболее общих и важных закономерностях в области предотвращения внештатных ситуаций в организационно-технических системах; знакомить их с современными техническими и программными средствами предотвращения внештатных ситуаций в организационно-технических системах.
2. Развивающая – научить студентов использовать полученные знания для решения прикладных функциональных и вычислительных задач будущей специальности.
3. Воспитательная – формировать на основе этих знаний естественно-научное мировоззрение, развивать способность к познанию и культуру мышления.

Требования к результатам освоения содержания дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО и ОПОП ВО по направлению подготовки (специальности) 27.05.01 «Специальные организационно-технические системы», специализации «Информационно-аналитическая деятельность в специальных организационно-технические системах»:

а) профессиональных (ПК):

способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ПК-7);

б) профессионально-специализированных (ПСК):

способен проводить системный анализ и моделирование программного обеспечения и средств безопасности специальных организационно-технических систем (ПСК-2.10).

В результате освоения дисциплины обучающийся должен получить следующие знания, умения и владения:

Знать:

- основные принципы разработки систем информационной безопасности (ПК-7);
- основные программные средства разработки систем информационной безопасности (ПК-7);
- принципы защиты конфиденциальной информации (ПК-7);
- принципы системной безопасности объектов специальных организационно-технических систем (ПСК-2.10);
- методы анализа рисков информационной безопасности (ПСК-2.10);
- принципы и методы обеспечения информационной безопасности объектов специальных организационно-технических систем (ПСК-2.10).

Уметь:

- определять объекты обеспечения информационной безопасности, оценивать основные параметры и свойства конфиденциальной информации (ПК-7);
- разрабатывать многоуровневые средства разграничения доступа к конфиденциальной информации (ПК-7);
- обеспечивать контроль соблюдения принципов информационной безопасности сотрудников, имеющих доступ к конфиденциальной информации (ПК-7);
- оценивать риски информационной безопасности, определять источники угроз (ПСК-2.10);
- разрабатывать модели обеспечения информационной безопасности (ПСК-2.10);
- обосновывать выбор методов и технологий обеспечения информационной безопасности (ПСК-2.10).

Владеть:

- навыками разработки и применения типовых компонентов систем информационной безопасности (ПК-7);
- навыками разработки типовых моделей обеспечения информационной

безопасности объектов специальных организационно-технических систем (ПСК-2.10).

Содержание и структура дисциплины (модуля)

Таблица 1 – Содержание разделов и формы текущего контроля

№ раздела	Наименование раздела	Содержание раздела
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы. Распространение объектно-ориентированного подхода на информационную безопасность. Наиболее распространенные угрозы	Понятие информационной безопасности. Основные составляющие. Важность проблемы. Основные термы и определения: информационная безопасность, защита информации, субъект информационных отношений, неприемлемый ущерб, поддерживающая инфраструктура, доступность, целостность, конфиденциальность, доктрина информационной безопасности РФ, компьютерное преступление, жизненный цикл информационных систем. Распространение объектно-ориентированного подхода на информационную безопасность. Сложные системы. Объектно-ориентированный подход. Определение класса, объекта, метода, Инкапсуляция, наследование, полиморфизм. Компонент, контейнер. Деление на субъекты и объекты. Троянские программы. Операционная система как сервис безопасности. Наиболее распространенные угрозы. Угроза, атака, уязвимость, окно опасности. Основные источники угроз. Злоумышленник, непреднамеренные ошибки, отказ пользователей, внутренний отказ. Вредоносное ПО: бомба, вирус, червь, троянская программа. Целостность данных, целостность программной среды
2	Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности. Административный уровень информационной безопасности	Законодательный уровень информационной безопасности. Комплексный подход к информационной безопасности. Законодательный уровень. Ограничительные меры, направляющие и координирующие меры. Право на информацию, право на личную и семейную тайну, банковская тайна, государственная тайна, коммерческая тайна, служебная тайна. Средства защиты информации. Информация, документированная информация. Документ. Информационные процессы, информационная система. Информационные ресурсы. Информация о гражданах, персональные данные. Конфиденциальная информация. Электронный документ. Электронная цифровая подпись. Корпоративная информационная система. План обеспечения ИБ, программа безопасности. Анализ рисков. Оценка уязвимостей. Нормативные документы. Стандарты и спецификации в области информационной безопасности. Безопасная система, доверенная система. Политика безопасности. Ядро безопасности. Оценочные стандарты и технические спецификации. Стандарт ISO/IEC 15408. Руководящие документы Гостехкомиссии России.

3	Управление рисками. Процедурный уровень информационной безопасности.	Административный уровень информационной безопасности. Основные понятия. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками. Основные понятия. Подготовительные этапы управления рисками. Основные этапы управления рисками.
4	Основные программно-технические мер. Экранирование, анализ защищенности. Идентификация и аутентификация, управление доступом. Биометрические средства доступа	Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Основные программно-технические меры. Основные понятия программно–технического уровня информационной безопасности. Архитектурная безопасность. Идентификация и аутентификация, управление доступом. Основные понятия. Парольная аутентификация. Одноразовые пароли. Управление доступом
5	Протоколирование и аудит, шифрование, контроль целостности. Криптографические средства	Протоколирование и аудит, контроль целостности. Основные понятия. Активный аудит. Контроль целостности. Цифровые сертификаты. Экранирование, анализ защищенности. Основные понятия. Архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности. Биометрические средства доступа. Основные понятия. Основные типы биометрических устройств. Криптографические средства. Основные понятия. Классификация криптографических средств. Современные алгоритмы шифрования.

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 специальности

27.05.01 Специальные организационно-технические системы

(код и наименование направления подготовки)

Настоящим подтверждаю, что представленный комплект аннотаций рабочих программ учебных дисциплин по специальности

27.05.01 Специальные организационно-технические системы

(код и наименование направления подготовки)

По специализации №2 Информационно-аналитическая деятельность в специальных организационно-технических системах

(наименование специализации)

Реализуемой по форме обучения Очная

Соответствует рабочим программам учебных дисциплин указанной выше образовательной программы.

Председатель НМС _____ С.С.Валеев

«30» августа 2016 г.