

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

«БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

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 «Безопасность критически важных информационных систем» является дисциплиной по выбору вариативной части основной профессиональной образовательной программы (ОПОП).

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.

Целью освоения дисциплины является подготовка специалистов, способных решать совокупность задач, связанных с сопровождением информационных систем, обладающая способностью сохранять критически важные данные и продолжать выполнять свои функции после массового (возможно, целенаправленного) уничтожения ее компонентов в результате различных катастрофических воздействий, как природного характера, так и инспирированных человеком, а в случае нарушения доступности системы за минимальное время восстановить свою работоспособность.

Задачи:

1. Сформировать знания об основных концепциях построения критически важной информационной системы.
2. Сформировать знания об основных методах и технологиях создания катастрофоустойчивых систем на различных этапах жизненного цикла с учетом требования законодательства и нормативных документов.
3. Сформировать знания основополагающих принципов оценки катастрофоустойчивости системы и математических методов, используемых при оценке катастрофоустойчивости информационных систем.
4. Сформировать знания о принципах и стратегии выбора наиболее эффективных катастрофоустойчивых решений.
5. Приобрести навыки применения методов повышения отказоустойчивости и катастрофоустойчивости информационных систем.
6. Сформировать знания об основных нормативно-правовых актах в области построения катастрофоустойчивой информационной системы.
7. Сформировать знания об основных нормативно-правовых актах в области сопровождения критически важных объектов инфраструктуры РФ.
8. Сформировать знания об управлении информационной безопасностью систем управления критически важными объектами инфраструктуры (АСУ ТП КВО).

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,	ОПК-7	- основные подходы исследования процессов обеспе-	- проводить обоснование и выбор рационального решения по	- системными правилами выявления причин нарушения

	подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		чения информации информационной безопасности	уровню защищенности информационной системы с учетом заданных требований	системных принципов функционирования объектов в области обеспечения информационной безопасности
2	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12	- основные организационные и правовые методы обеспечения безопасности информационных систем	- разрабатывать предложения по совершенствованию управления безопасностью информационных систем и сетей; - организовать работу коллектива по проведению научных исследований в области информационной безопасности	- методами анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области информационной безопасности; - навыками организации работы коллектива по проведению научных исследований в области информационной безопасности
3	Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	ПСК-3	- современные методы защиты локальной и удаленной вычислительных сетей	- разрабатывать и исследовать методы защиты локальной и удаленной вычислительных сетей; - проводить анализ безопасности информационных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности; - разрабатывать математические модели отдельных средств защиты информации, а также модели безопасности защищаемых информационных систем в целом	- навыками применения организационных и правовых мер для обеспечения безопасности информационных систем; - навыками применения современных методов защиты локальной и удаленной вычислительных сетей; - навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в информационных системах

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	Критически важные объекты 1. Безопасность критической инфраструктуры государства 2. Критические важные объекты инфраструктуры (КВО) 3. Современная концепция создания комплексных систем безопасности КВО инфраструктуры 4. Категорирование объектов КИИ в РФ 5. Критическая информационная инфраструктура РФ (КИИ) 6. Ключевая (критически важная) система информационной инфраструктуры (КСИИ) 7. Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры РФ (АСУ КВО)

№	Наименование и содержание разделов
2	Основные понятия катастрофоустойчивости информационной системы (ИС) 1. Понятия катастрофоустойчивости, живучести и отказоустойчивости 2. Информационные системы. 3. Виды, архитектура, субъекты и объекты взаимодействия. 4. Модель катастрофических воздействий 5. Моделирование и прогноз природных и техногенных катастроф. 6. Уровни катастрофоустойчивости 7. Показатели и критерии функционирования катастрофоустойчивой информационной системы. 8. Живучесть информационных систем 9. Отказоустойчивость и надежность. 10. Разработка моделей оценки живучести ИС
3	Модели и показатели функционирования катастрофоустойчивых ИС 1. Модель оценки информационной системы с позиции доступности 2. Модель оценки информационной системы по уровням катастрофоустойчивости 3. Модель оценки информационной системы с позиции живучести 4. Оценка эффективности катастрофоустойчивых решений 5. Структурный анализ катастрофоустойчивой ИС
4	Методы обеспечения катастрофоустойчивости ИС 1. Методика создания катастрофоустойчивой информационной системы 2. Классификация методов обеспечения катастрофоустойчивости 3. Стратегии резервирования 4. Кластеризация 5. Избыточные структуры 6. Резервные центры обработки данных. 7. Выбор варианта катастрофоустойчивой конструкции центра обработки информации 8. Выбор стратегии восстановления в катастрофоустойчивой системе 9. Разработка модели оценки доступности информации в катастрофоустойчивых системах 10. Исследование готовности и доступности ИС 11. Исследование уровней катастрофоустойчивости на моделях типовых ИС 12. Моделирование дестабилизирующих воздействий и их последствий на ИС 13. Разработка модели оценки катастрофоустойчивых решений
5	ИБ систем управления КВО 1. Политика Российской Федерации в обеспечении безопасности КВО 2. Место СУИБ в общей системе менеджмента критически важным объектом 3. Оценка безопасности АСУ ТП критической инфраструктуры 4. Процесс формирования режима безопасности АС 5. Этапы ЖЦ регулятора безопасности АС 6. Пример типовой структуры защищённой АСУ ТП

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.