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 – 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 «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 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.

Целью освоения дисциплины является формирование понятийного аппарата, методологической базы, учитывающей специфику защиты информации в правоохранительной сфере, систематизированных и структурированных знаний о принципах и особенностях функционирования системы защиты информации в критически важных информационных системах, способах и средствах защиты информации на критически важных объектах.

Задачи:

– сформировать знания о критически важных информационных системах (КВИС) как об объектах защиты, об их специфике и особенностях, по сравнению с традиционными информационными системами;

– проанализировать основные отечественные и зарубежные нормативные правовые документы, а также методические рекомендации в области безопасности КВИС;

– изучить факторы, затрудняющие обеспечение должного уровня защищенности КВИС;

– изучить возможные источники угроз, угрозы и объекты атаки КВИС, а также наиболее уязвимые с точки зрения информационной безопасности компоненты критически важных объектов, научиться грамотно составлять модель нарушителя и модель угроз в соответствии с особенностями критически важных объектов (КВО), бизнес-процессы которых поддерживает КВИС;

– изучить особенности построения системы защиты информации КВИС, мероприятия, направленные на повышение уровня защищенности КВО, а также специализированные средства защиты информации автоматизированной системы управления технологическими и производственными процессами критически важных объектов (АСУ ТП КВО);

– сформировать общее представление у студентов о катастрофоустойчивости современных информационных систем;

– изучить способы обеспечения целостности и доступности в критически важных информационных системах, а также современные отечественные и зарубежные средства резервирования ресурсов и данных;

– изучить элементы типовой структуры защищенной критически важной информационной системы и способы их реализации.

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 выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	ОПК-1	– определения и структуру КВО, КВИС, АСУ ТП КВО в соответствии с нормативной правовой базой РФ; – основные принципы безопасности КВИС; – статистику по инцидентам в области обеспечения безопасности КВИС; – разделы федерального плана по повышению уровня защищенности КВО.	– строить модель нарушителя КВО в соответствии с квалификацией нарушителей и злоумышленников; – строить модель угроз КВО в соответствии с угрозами нарушения доступности и целостности информации – работать с международной базой данных уязвимостей (NVD) и банком данных угроз безопасности информации ФСТЭК.	- методами выявления угроз и численными методами оценивания рисков нарушения информационной безопасности КВИС и АСУ ТП КВО – методикой оценки уязвимостей и методикой построения вектора атаки на КВИС.
2	Способность принимать участие в создании системы защиты информации на объекте информатизации	ПК-31	– общие методы построения архитектуры сети критически важного объекта, основные контуры сети КВИС; – специфические методы и средства защиты информации на критически важных объектах; – факторы, затрудняющие обеспечение должного уровня защищенности КВО.	– выявлять уязвимости КВИС и АСУ ТП КВО; – определять наиболее уязвимые компоненты инфраструктуры КВО и критически важной информационной системы; – определять требуемый уровень защищенности КВИС в соответствии с нормативными правовыми актами РФ.	– методами отнесения объектов к критически важным объектам; – методиками оценки защищенности критически важного объекта; – специальными способами защиты инфраструктуры КВО.
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	– перечень мероприятий, направленных на повышение защищенности КВО; – типовую структуру защищенной КВИС; – отечественную и зарубежную нормативную правовую базу в области обеспечения безопасности критически важных объектов.	– применять технологии архивации и резервного копирования, реализованные в современных версиях операционных систем; – настраивать и работать с отказоустойчивыми кластерами.	– методами реализации системы защиты информации в АСУ ТП КВО; -методами построения катастрофоустойчивых центров обработки данных; - методами оценки рисков доступности и целостности КВИС и информационным активам КВО;

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	**Основные сведения о КВИС как об объекте защиты:** 1) Определения КВО, КВИС, АСУ ТП КВО согласно различным нормативным правовым актам. Связь основных элементов КВО. Перечень критически важных объектов РФ. Международная статистика успешных атак на КВО. 2) Классификация КВО по значимости и по уровням угроз. Разделы федерального плана повышения защищенности КВО. 3) Методика отнесения объектов защиты к критически важным объектам.
2	**Нормативная правовая база РФ в области обеспечения безопасности КВО:** 1) Основные нормативные документы в области защиты КВО. Приказ ФСТЭК № 31 от 14.03.2014 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Требования к средствам защиты в соответствии с классом защищенности АСУ ТП КВО. 2) Методика построения плана повышения защищенности критически важного объекта. Методика оценки защищенности критически важного объекта.
3	**Архитектура сети критически важного объекта и ее уязвимости:** 1) Основные контуры топологии сети критически важного объекта. Основные элементы АСУ ТП КВО. 2) Угрозы и уязвимости, специфичные для КВО и АСУ ТП КВО. Наиболее уязвимые компоненты инфраструктуры КВО. Классы угроз АСУ ТП КВО. 3) Факторы, затрудняющие обеспечение должного уровня защищенности КВИС.
4	**Модель угроз критически важного объекта:** 1) Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры. Табличный вид базовой модели угроз в соответствии с базовой моделью угроз ФСТЭК для КВО. 2) Описание процесса моделирования угроз безопасности информации в КВО. Объекты атаки в КВИС. Критичность ресурсов КВИС. Модель нарушителя КВИС. 3) Модель угроз КВИС в виде нечеткой когнитивной карты. Источники угроз, объекты атак и компоненты инфраструктуры КВИС. Методика расчета вероятности реализации угрозы КВИС на основе модели угроз в виде нечеткой когнитивной карты. 4) Методика оценки уязвимостей КВИС по стандарту CVSS. Векторы атаки в соответствии с методикой CVSS. Базовые, временные и контекстные метрики. Банк данных угроз и уязвимостей ФСТЭК.
5	**Специальные средства защиты ИТ-инфраструктур КВО:** 1) Реализация системы защиты информации в АСУ ТП КВО. Мероприятия, направленные на повышение защищенности КВО. Построение системы защиты информации КВИС. Типовая структура защищенной КВИС. 2) Специальные средства повышения надежности инфраструктуры КВИС. Катастрофоустойчивость информационной системы КВО. Методики обеспечения отказоустойчивости. Специальные средства, обеспечивающие отказоустойчивость КВИС. Методика многокритериального выбора средств обеспечения надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации в КВИС.

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.