

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
«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»**

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

Место дисциплины в структуре образовательной программы

Дисциплина «Программно аппаратные средства защиты информации» является дисциплиной базовой части.

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 (ОПОП).

Целью освоения дисциплины является формирование систематизированных знаний о роли программно-аппаратной защиты компьютерной информации, об основных моделях угроз информационной безопасности, принципах, методах и направлениях программно-аппаратной защиты информации.

Задачи:

- сформировать знания о назначении, составе и принципах работы программно-аппаратных средств защиты компьютерной информации;
- изучить основные технические характеристики и особенности эксплуатации программных и аппаратных средств защиты компьютерной информации;
- изучить правовую и нормативную базу, регламентирующую использование программно-аппаратных средств защиты информации;
- сформировать навыки использования программных и аппаратных средств защиты информации для реализаций политики информационной безопасности.

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, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования	ОПК-7	основные методы исследования ПО и защиты его исследования	осуществлять защиту программного обеспечения от несанкционированного копирования и использования	навыками применения антивирусных программ
2	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-	ПК-1	основы симметричной криптографии, отечественный стандарт по симметрич-	настраивать ключевую систему шифраторов «Криптон», осуществлять ее настройку при	навыками администрирования криптосистем с закрытыми ключами

	аппаратных (в том числе криптографических) и технических средств защиты информации		ной криптографии, ключевую систему шифраторов Криптон	централизованной и распределенной структуре организации	
3	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2	основы криптографии с открытыми ключами алгоритмов и стандарты электронной подписи и хеш-функций; принципы реализации стеганографического упрятывания информации	осуществлять защиту информации с использованием криптосистем с открытыми ключами; реализовывать защиту авторских прав с помощью водяных знаков	навыками администрирования криптографических систем с открытыми ключами; навыками работы со стеганографическими программами и программами создания водяных знаков
4	Способность администрировать подсистемы информационной безопасности объекта защиты	ПК-3	классификацию компьютерных вирусов и антивирусных средств	использовать весь спектр методов защиты от разрушающих программных воздействий	навыками применения антивирусных программ
5	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	ПСК-2	основные направления и методы защиты от несанкционированного копирования и утечек информации	осуществлять администрирование DLP систем	навыками выявления утечек информации, расследования компьютерных инцидентов

Содержание разделов дисциплины

№	Наименование и содержание раздела
1	Программные и аппаратные средства криптографии с закрытым ключом Понятие симметричной криптографии. Порядок использования крипто средств в России. Требования к сертификации средств шифрования. Понятие шифровальных средств. Программные и аппаратные средства семейства Криптон. Программные и аппаратные средства прозрачного шифрования информации. Технологии восстановления ключей
2	Программные и аппаратные средства шифрования с открытым ключом Понятие асимметричной криптографии. Практическая схема использования криптографии с открытыми ключами для шифрования данных. Хэш-функции и их использование в программно-аппаратных средствах защиты информации. Практические способы и средства реализации электронной подписи. Сертификаты открытых ключей. Стандарт X509. Понятие CRL. Функции сертификационного агентства, обязанности, оказываемые услуги. Протокол SSL, TLS. Организация работы. Отечественные продукты шифрования с открытым ключом.
3	Стеганография Понятие стеганографии. Базовые принципы компьютерной стеганографии Понятие суррогатной, селективирующей, конструирующей стеганография. Поточковые контейнеры и контейнеры случайного доступа. Их достоинства и недостатки. Водяные знаки, их назначение и использование. Стеганографические программы. Программы создания и проверки водяных знаков
4	МетодыЗИ от НСД

	Руководящие документы ФСТЭК по защите от НСД информации. Потенциальные угрозы информации, обрабатываемой в ПК. Возможные каналы НСД. Методы аутентификации пользователей. Основные электронные идентификаторы. Биометрическая аутентификация. Сравнительная характеристика разных биометрических методов идентификации. Основные показатели для оценки эффективности методов идентификации пользователей. Архитектура и основы организации систем защиты информации на ПК. Основные программно-аппаратные комплексы защиты информации. Реализация дискреционного и мандатного разграничения доступа, аудита, контроля целостности. Защищенные компьютеры. Методы защиты компьютерной техники от краж
5	Исследование ПО, защита ПО от исследования Методы исследования ПО. Способы защиты программ от исследования. Механизмы защиты от отладчиков. Механизмы защиты от дизассемблеров. Руководящий документ ФСТЭК. "Классификация по уровню контроля отсутствия не декларированных возможностей".
6	Защита от несанкционированного копирования. Защита от несанкционированного копирования ПО, распространяемого на CD и DVD. Структура данных на CD, DVD дисках. Интерфейсы взаимодействия с оборудованием. Методы и приемы защиты CD, DVD от копирования. Защита от пофайлового копирования. Промышленные системы защиты CD от несанкционированного копирования Активация программного обеспечения. Электронные ключи. Понятие электронного ключа. Принципы работы. Классификация. Этапы развития. Достоинства электронных ключей. Классификация. Защита данных. Защита в сети. RMS, IRM системы. DLP системы
7	Компьютерные вирусы и борьба с ними Разрушающие программные воздействия. Понятие компьютерного вируса. Пути проникновения. Основные виды. Цикл жизни. Устойчивость операционных систем к вирусам. Механизм заражения вирусом. Загрузочные вирусы. Файловые вирусы. Резидентные вирусы. Сетевые вирусы. Макровирусы.

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.