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-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ»***

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 «Програмнно аппаратная защита информации» является дисциплиной базовой части.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 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 (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 средствах 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.

## 2. 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 формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечить комплексную защиту информации и сведений, составляющих государственную тайну, но объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз | ПК-1 | основы криптографии с открытыми ключами алгоритмв и стандарты электронной подписи и хеш-функций | осуществлять защиту информации с использованием криптосистем с открытыми ключами | навыками администрирования криптографических систем с открытыми ключами |

| | | | | | |
|---|---|---|---|---|---|
| 2 | способность применять технические и программные средства обработки и защиты информации | ПК-2 | основы симметричной криптографии, отечественный стандарт по симметричной криптографии, ключевую систему шифраторов Криптон; принципы реализации стеганограческого упрятывания информации | настраивать ключевую систему шифраторов «Криптон», осуществлять ее настройку при централизованной и распределенной структуре организации; реализовывать защиту авторских прав с помощью водяных знаков | навыками администрирования криптосистем с закрытыми ключами<br><br>навыками работы со стеганографическими программами и программами создания водяных знаков |
| 3 | способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации | ПК-4 | нормативные документа в области защиты информации от несанкционного доступа (стандарты, СТР-к, руководящие документы, приказы и методические документы ФСТЭК) | использовать в профессиональной деятельности нормативные правовые акты и методические документы в области защиты информации и обеспечения информационной безопасности | навыками установки и эксплуатации систем контроля и разграничения доступа |
| 4 | способность осуществлять администрирование подсистем обеспечения информационной безопасностью объекта информатизации | ПК-6 | классифкацию компьютерных вирусов и антивирусных средств | использовать весь спектр методов защиты от разрушающих программных воздействий | навыками применения антивирусных программ |
| 5 | способность принимать участие в создании системы защиты информации на объекте информатизации | ПК-31 | основные методы исследования ПО и защиты его исследования; основные направления и методы защиты от несанкциони-рованного копирования и утечек информации | осуществлять защиту программного обеспечения от несанкционированного копирования и использования осуществлять администрирование DLP систем | методами защиты программного обеспечения (ПО) от изучения и обратного проектирования ;<br>навыками выявления утечек информация, расследования компьютерных инцидентов |

## Содержание разделов дисциплины

| № | Наименование и содержание раздела |
|---|---|
| 1 | **Программные и аппаратные средства криптографии с закрытым ключом**<br>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**<br>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, селектирующей, конструирующей стеганография. Потоковые контейнеры и контейнеры случайного доступа. Их достоинства и недостатки. Водяные знаки, их назначение и использование. Стеганографические программы. Программы создания и проверки водяных знаков |
| 4 | **Методы ЗИ от НСД**<br>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 дискреционное и мандатного разграничения доступа, аудита, контроля целостности. Защищенные компьютеры. Методы защиты компьютерной техники от краж |
| 5 | **Исследование ПО, защита ПО от исследования**<br>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<br>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.<br>DLP системы |
| 7 | **Компьютерные вирусы и борьба с ними**<br>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.