

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

«ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

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 «Защита информационных процессов в компьютерных системах» является дисциплиной вариативной части.

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 (ОПОП).

Целью освоения дисциплины является формирование систематизированных знаний о роли защиты информационных процессах в компьютерных системах и сетях, об основных моделях угроз информационной безопасности, принципах, методах и направлениях защиты информации в компьютерных системах и сетях.

Задачи:

- сформировать знания о назначении, составе и принципах работы средств защиты информации в компьютерных системах;
- изучить основные технические характеристики и особенности эксплуатации сетевых средств защиты компьютерной информации;
- изучить правовую и нормативную базу, регламентирующую использование сетевых средств защиты информации;
- сформировать навыки использования сетевых средств защиты информации для реализации политики информационной безопасности компьютерных систем и сетей.

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, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ПК-1	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ, ФСТЭК в области защиты информации в корпоративных сетях.	формировать и настраивать политику безопасности и систему разграничения доступа в корпоративных системах на базе Linux	методикой анализа сетевого трафика, результатов работы систем обнаружения вторжений

2	Способность применять технические и программно-аппаратные средства обработки и защиты информации	ПК-2	принципы построения системы защиты в сетях Windows	разрабатывать, администрировать подсистемы безопасности и оценивать защищенности компьютерных систем	Навыками конфигурирования параметров безопасности операционной системы Windows
3	Способность принимать участие в создании системы защиты информации на объекте информатизации	ПК-31	принципы и методы реализации виртуальных частных сетей	Выбрать оптимальный уровень модели OSI для реализации VPN, произвести оптимальный выбор VPN решений.	Навыками конфигурирования VPN каналов
4	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ПСК-1	механизмы обеспечения безопасности информационных процессов в глобальных сетях.	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты информации.	методами защиты мобильных пользователей

Содержание разделов дисциплины

№	Наименование и содержание раздела
1	Защита информационных процессов в операционных системах Windows Основные компоненты системы безопасности Windows. Их назначение и взаимодействие. Проверка подлинности пользователей при входе в систему Windows при локальном и доменном входе. Идентификаторы безопасности, их структура и виды. Маркеры и субъекты доступа. Олицетворение и его уровни. Диспетчер учетных записей. Организация хранения паролей. Шаблоны безопасности. Групповые политики. Предотвращение выполнения данных (DEP). Контроль учетных записей (UAC). Родительский контроль. Applocker. Технология защиты ядра от изменения. Windows Resource Protection. Рандомизация компоновки адресного пространства (ASLR). Разграничение доступа. Списки контроля доступа. Их структура и управление. Организация доступа к сетевым ресурсам. Протокол SMB. Файловая система шифрования. Bitlocker. Шифрование логических дисков и сменных дисков. Организация аудита. Структура реестра. Защита удаленного и терминального доступа. Протокол аутентификации Kerberos: механизм работы, подпротоколы, структура билетов.
2	Защита информационных процессов в Linux Организация хранения аутентификационной информации. Типы пользователей. Группы. Организация разграничения доступа. Права доступа, атрибуты.
3	Межсетевые экраны Понятие, причины использования, классификация, особенности и принципы работы. Руководящий документ ФСТЭК.
4	Виртуальные частные сети (VPN) Принципы и способы реализации, решаемые задачи, области применения, требования. Защищенные каналы на разных уровнях моделях OSI. Достоинства и недостатки. Схемы взаимодействия с провайдером при реализации VPN. Семейство протоколов IPSec. Состав, схемы и режимы работы. Протокол IKE: этапы и режимы функционирования, способы аутентификации. Семейство протоколов SSL/TLS. Структура пакетов. Функции основных подпротоколов. Организация аутентификации и шифрования. Способы обмена ключами. Протокол SOCKS, схема установления соединения, особенности работы SOCKS. Особенности реализации защищенных соединений на канальном уровне. Протокол PPTP. Принципы работы. Структура пакетов. Схемы применения Протокол L2F, L2TP. Сравнительный анализ PPTP, L2F, L2TP. Протокол SSTP. Direct Access. Назначение, особенности, достоинство, механизмы работы, способы подключения клиентов. Технология BranchCache.

5	<p>Системы обнаружения вторжений Типовые удаленные атаки: классификация, характеристика, механизмы реализации, Этапы реализации. Средства анализа защищенности. Системы обнаружения вторжений системного и сетевого уровня, их размещение, достоинства и недостатки. Обманные системы, их классификация и особенности.</p>
6	<p>Защита информационных процессов в беспроводных сетях Протокол WEP. Реализация шифрования и контроля целостности/Аутентификация пользователей. Атаки на протокол WEP. Стандарт аутентификации 802.1х. TKIP, MIC. Управление ключами в WPA. Особенности WPA2. Методы защиты информации в сетях сотовой связи (GSM, CDMA, Bluetooth, 3G, 4G).</p>

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.