Негосударственное образовательное учреждение
высшего образования
Московский технологический институт

«УТВЕРЖДАЮ»
Директор колледжа
_____ Куклина Л. В.
«24» июня 2016 г.

АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Специальность

10.02.01 Организация и технология защиты информации

Уровень подготовки

Базовый

Квалификация выпускника

Техник по защите информации

Москва – 2016

1. Цели и задачи освоения дисциплины

Целями освоения дисциплины является:
обучение принципам построения систем защиты информации в операционных системах, на рабочих станциях и персональных компьютерах, в вычислительных сетях и системах управления базами данных.

Задачи освоения дисциплины состоят в следующем:

- изучение основ построения подсистем защиты информации в автоматизированных системах различной архитектуры;
- освоение принципов функционирования современных систем идентификации и аутентификации;
- изучение принципов построения и использования межсетевых экранов; изучение основ построения систем безопасности в вычислительных сетях.

2. Место дисциплины в структуре ППССЗ СПО

а) дисциплина относится к циклу Профессиональные модули и является одним из основных курсов специальной профессиональной подготовки.
б) Настоящему курсу должно предшествовать изучение следующих дисциплин: «Основы информационной безопасности», «Технические средства информатизации», «Основы объектно-ориентированного программирования».
б) знание дисциплины поможет осуществить действия по обеспечению деятельности организации, она связана с правовыми, социально-психологическими, эко¬номическими и техническими дисциплинами, дисциплинами по теории и методологии защиты информации, дисциплинами документоведения и др.

3.Тематическое содержание дисциплины

Тема 1. Назначение и функции программно-аппаратных средств обеспечения безопасности
Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Эскалация привилегий. Функции программно-аппаратных средств защиты информации. Содержание и задачи процесса обеспечения информационной безопасности с использованием программно-аппаратных средств.
Тема 2. Методы защиты информации от несанкционированного доступа
Требования к специализированным средствам защиты информации от несанкционированного доступа. Контроль целостности системного программного обеспечения и аппаратных средств. Организация виртуальных логических дисков. Шифрование пользовательских виртуальных дисков. Формирование ключевой информации.
Тема 3. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем
Средства обеспечения целостности составных частей компьютера.

Защита узлов и блоков компьютеров от несанкционированного доступа. Средства контроля доступа к рабочему месту пользователя. Программные средства выявления фактов физического доступа к системному блоку и узлам автоматизированной системы.

Тема 4. Анализ уязвимости программного обеспечения автоматизированных систем

Типовая структура подсистемы безопасности ОС и выполняемые ей функции: идентификация и аутентификация, разграничение доступа, аудит, подотчетность действий, повторное использование объектов, точность и надежность обслуживания, защита обмена данных. Реализация подсистем безопасности и средства обеспечения безопасности в ОС семейств UNIX и Windows. Домены безопасности критерии защищенности ОС.

Понятие вредоносного кода. Программные закладки. Классификация программных закладок. Предпосылки к внедрению программных закладок. Уязвимости программного обеспечения. Принципы построения политики безопасности. Уязвимости политики безопасности. Человеческий фактор. Сокрытие программных закладок.

Тема 5. Методы защиты от вредоносных программ

Сигнатурное и эвристическое сканирование. Аппаратные средства противодействия вредоносному коду. Контроль целостности программного обеспечения. Мониторинг информационных потоков. Изолированная программная среда. Цифровая подпись исполняемого кода. Шифрование исполняемого кода. Средства анализа уязвимостей.

Тема 6. Средства идентификация и аутентификации пользователей автоматизированных систем

Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях протоколы аутентификации при удаленном доступе средства и методы обеспечения целостности и конфиденциальности защита серверов и рабочих станций средства защиты локальных сетей при подключении к Интернет защитные экраны защита виртуальных локальных сетей.

Применение парольных систем. Аутентификация с помощью физических предметов хранящихся у пользователя. Электронные ключи. Пластиковые карты.