

Аннотация рабочей программы дисциплины (модуля)
Б1.В.ДВ.09.01 Защита сетей от внешних угроз

Целями освоения дисциплины Б1.В.ДВ.09.01 Защита сетей от внешних угроз» являются формирование профессиональных компетенций будущих специалистов в области Информационных систем и технологий, формирование у студентов базовых знаний, умений и навыков по основам защиты компьютерных сетей от внешних угроз при помощи программно-аппаратных средств достаточных для освоения основной профессиональной образовательной программы направления 09.03.02 Информационные системы и технологии.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. Формирование представления и получение навыков работы с программно-аппаратными средствами защиты информации, реализующим отдельные функциональные требования по защите.
2. Формирование базовых знаний и умений разработки компонентов программно-аппаратных средств защиты информации.
3. Формирование базовых знаний по методам и средствам хранения ключевой информации, методам и средствам ограничения доступа к компонентам вычислительных систем, задачам и технологии сертификации программно-аппаратных средств защиты информации на соответствие требованиям информационной безопасности.
4. Формирование базовых знаний и умений по методам защиты от вредоносных программ, защите программ от изменения и контролю целостности.

Формируемые компетенции и индикаторы их достижения по дисциплине:

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПКС-2	ПКС-2. Способен проводить формализацию предметной области с целью создания информационной системы	ПКС-2.1 - Знает требования к компьютерному программному обеспечению; виды технической спецификации на программные компоненты и их взаимодействие; методы проектирования компьютерного программного обеспечения ПКС-2.2 – Умеет применять требования к компьютерному программному обеспечению; разрабатывать технические спецификации на программные компоненты и их взаимодействие; применять методы проектирования компьютерного программного обеспечения; ПКС-2.3 – Владеет методами разработки требований к компьютерному программному обеспечению, технических спецификаций на программные компоненты, методами проектирования компьютерного программного обеспечения.

ПКС-3	ПКС-3 - Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС	ПКС-3.1 - Знает методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.2 - Умеет применять методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.3 - Владеет методами организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС.
-------	---	--

Содержание дисциплины

Раздел 1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.

Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Модель компьютерной системы. Понятие монитора безопасности. Концепция диспетчера доступа. Обеспечение гарантий выполнения политики безопасности. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды

Раздел 2 Программно-аппаратные средства обеспечения информационной безопасности.

Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем. Средства обеспечения информационной безопасности в операционной системе GNU/Linux. Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в операционной системе GNU/Linux. Замкнутая программная среда и контроль целостности в операционной системе GNU/Linux. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от изменения и контроль целостности.

Раздел 3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.

Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий

Темы и планы лабораторных занятий

Тема 1. Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в операционной системе.

Тема 2. Замкнутая программная среда и контроль целостности в операционной системе

Тема 3. Разработка защищенного ПО с применением аппаратных ключей eToken
Знакомство с eToken API

Тема 4. Разработка защищенного ПО с применением аппаратных ключей eToken
Работа с сертификатами X.509 на eToken

Тема 5. Разработка защищенного ПО с применением аппаратных ключей eToken.
Объекты eToken.

Тема 6. Разработка защищенного ПО с применением аппаратных ключей eToken.
Шифрование данных с помощью eToken.

Тема 7. Защита автоматизированных систем от вредоносного программного обеспечения»