

Аннотация рабочей программы дисциплины (модуля)
Б1.О.27 Программно-аппаратные средства защиты информации

Целями освоения дисциплины **«Б1.О.26 Программно-аппаратные средства защиты информации»** являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

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
ОПК-4.	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1 - Знает основные физические законы, физическую сущность явлений и процессов; ОПК-4.2 - Умеет использовать математические модели физических явлений и процессов; ОПК-4.3 - Владеет практическими навыками решения типовых прикладных физических задач.
ОПК-6.	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации

		ограниченного доступа.
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

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 APIT

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»