АННОТАЦИЯ

Дисциплины

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем».

Специализация «Информационная безопасность автоматизированных систем на транспорте».

Квалификация выпускника – специалист по защите информации.

**1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Программно-аппаратные средства информационной безопасности» (Б1.Б.17) относится к базовой части профессионального цикла и является обязательной дисциплиной.

**2. Цель и задачи дисциплины**

Цель изучения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» состоит в изучении основных принципов создания программно-аппаратных средств обеспечения информационной безопасности, концепции диспетчера доступа; программно-аппаратных средств, реализующих отдельные функциональные требования по защите, их принципов действия и технологических особенностей, взаимодействия с общесистемными компонентами вычислительных систем; методов и средств ограничения доступа к компонентам вычислительных систем; методов и средств привязки программного обеспечения к аппаратному окружению и физическим носителям; методов и средств хранения ключевой информации; защиты программ от изучения, способов встраивания средств защиты в программное обеспечение; защиты от разрушающих программных воздействий, защиты программ от изменения и контроль целостности, построения изолированной программной среды; задач и технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основных категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратных средств защиты информации в сетях передачи данных..

Для достижения поставленной цели решаются следующие задачи:

* Знакомство с основами создания программно-аппаратных средств обеспечения информационной безопасности;
* Изучение концепций построения диспетчеров доступа;
* Изучение взаимодействия программно-аппаратных средств обеспечения информационной безопасности с общесистемными компонентами вычислительных систем;
* Изучение методов и средств ограничения доступа к компонентам вычислительных систем.

**3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующихкомпетенций-ОПК-8,ПК-6,ПК-26

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

* основные принципы создания программно-аппаратных средств обеспечения информационной безопасности;
* концепции построения диспетчера доступа;
* методы и средства ограничения доступа к компонентам вычислительных систем;
* методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям;
* методы и средства хранения ключевой информации;
* способы встраивания средств защиты в программное обеспечение;
* основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.

**УМЕТЬ*:***

* использовать на практике, основные, представленные на рынке, аппаратно-программные средства обеспечения информационной безопасности;
* выполнять привязку программного обеспечения системы защиты информации к аппаратному окружению и физическим носителям;
* использоватьтехническую документацию для корректной и непротиворечивой настройки механизмов безопасности программно-аппаратных средств обеспечения информационной безопасности;
* использовать средства хранения ключевой информации и способы встраивания аппаратных компонентов средств защиты в программное обеспечение;
* оценивать эффективность и надежность функционирования программно-аппаратных средств обеспечения информационной безопасности;
* выявлять уязвимости защиты программно-аппаратных средств обеспечения информационной безопасности и предотвращать их использование для взлома защиты;
* разрабатывать предложения по совершенствованиюприменения программно-аппаратных средств обеспечения информационной безопасности на предприятии.

**ВЛАДЕТЬ:**

* навыками администрирования программно-аппаратных средств обеспечения информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;
* профессиональной терминологией в области программно-аппаратных средств обеспечения информационной безопасности;
* навыками корректного использования программно-аппаратных средств обеспечения информационной безопасности.

**4. Содержание и структура дисциплины**

Требования к защите компьютерной информации.

Анализ защищенности современных ОС.

Подходы к проектированию СЗИ.

Оценивание эффективности СЗИ при их проектировании.

Проектирование СЗИ.

Системный подход к проектированию систем защиты.

Архитектура СЗИ.

Особенности архитектуры сетевой СЗИ.

Анализ эффективности СЗИ.

Авторизация и ее задачи.

Добавочные механизмы парольной защиты.

Добавочные механизмы парольной защиты.

Классификация объектов и субъектов доступа.

Канонические модели управления доступом.

Реализация моделей доступа.

Общие положения по реализации управления доступом.

Особенности настройки механизмов управления доступом.

Субъект доступа «Процесс».

Особенности разграничения доступа к разным ресурсам.

Локализация прав доступа и практические примеры управления доступом.

Особенности использования субъекта «процесс» и организация замкнутой программной среды.

Формальная модель диспетчера доступа.

Моделирование рабочей станции без системы защиты.

Моделирование рабочей станции с системой защиты.

Влияние добавочных средств на загрузку вычислительной системы.

Механизм контроля целостности.

Использование аппаратных средств защиты.

Противодействие переводу программного обеспечения СЗИ в пассивное состояние.

**5. Объем дисциплины и виды учебной работы**

Объем дисциплины – 5 зачетных единиц (180 час.), в том числе:

лекции – 34 час.

практические занятия – 16 час.

лабораторные работы – 34 час.

самостоятельная работа – 60 час.

контроль – 36 час.

форма контроля знаний –экзамен (7 семестр), зачет (8 семестр).