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

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 следующих **общепрофессиональных компетенций (ОПК)**:

* способности к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК):**

* способности проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
* способности администрировать подсистему информационной безопасности автоматизированной системы (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;
* использовать техническую 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 совершенствованию применения 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**

Наименование разделов 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 – 32 час.

практические занятия – 16 час.

лабораторные работы – 32 час.

самостоятельная работа – 60 час.

Форма контроля знаний – экзамен (VII семестр), зачет (VIII семестр).