Аннотация к рабочей программе дисциплины

«Теория и проектирование защищённых систем»

Рабочая программа учебной дисциплины «Теория и проектирование защищенных систем» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин вариативной части учебного плана Б1.В.04.

Трудоемкость дисциплины составляет 5 зачетных единиц, в академических часах – 180 часов. Среди них на лекции выделено 36 часов, лабораторные работы 36 часа, самостоятельную работу студента 72 часа, а также 36 часов на подготовку к экзамену. Дисциплина реализуется на 5 курсе в А семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теория и проектирование защищенных систем» логически и содержательно связана с такими курсами, как «Информатика», «Основы информационной безопасности», «Компьютерные сети», «Аппаратные средства вычислительной техники».

В курс лекций включены такие темы как: «Основные понятия и определения», «Проектирование систем в защищенном исполнении», «Модели угроз», «Создание систем защиты персональных данных», «Основные категории средств защиты ИСПДн» и др.

Цель изучения дисциплины «Теория и проектирование защищённых систем» заключается в изучении основных понятий, методологии и практических приемов проектирования, разработки и внедрения автоматизированных систем на предприятиях различных отраслей промышленности с учетом требований по обеспечению информационной безопасности.

Задачи дисциплины**:**

– приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области защиты автоматизированных систем;

– формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.

Для успешного изучения дисциплины «Теория и проектирование защищенных систем» у обучающихся должны быть сформированы следующие предварительные компетенции:

– способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

– способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

– способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);

– способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);

– способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-6 – способность участвовать в разработке проектной и технической документации	Знает	защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и ассиметричных криптографических алгоритмов; математические модели шифров
	Умеет	формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и ассиметричные криптографические алгоритмы; осуществлять меры противодействия нарушениями сетевой безопасности с использованием различных программных и аппаратных средств защиты
	Владеет	навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространённых семейств; навыками анализа программных реализаций
ПК-7 – способность проводить анализ проектных решений по обеспечению защищенности	Знает	защитные механизмы и средства обеспечения безопасности операционных систем; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в стеях, реализующих протоколы интернет транспортного

компьютерных систем		и сетевого уровня; основные проколы индентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений
	Умеет	формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе
	Владеет	навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией)
ПК-8 – способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знает	защитные механизмы и средства обеспечения безопасности операционных систем; основные средства и методы анализа программных реализаций; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня
	Умеет	применять защищённые протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе
	Владеет	навыками анализа программных реализаций; криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками настройки межсетевых экранов; навыками конфигурирования локальных

		компьютерных сетей. реализации сетевых протоколов с помощью программных средств

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория и проектирование защищенных систем» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).