Аннотация к рабочей программе дисциплины
Автор: Урбан В.А.
Наименование дисциплины: Б1.В.ДВ.06.02 Системы обнаружения вторжений
Цель освоения дисциплины:

- изучение основных принципов, методов и средств защиты информации в процессе ее обработке, хранении и передачи с использованием компьютерных средств в информационных системах;

- теоретическое и практическое обучение студентов методам и средствам выявления и блокирования каналов утечки информации.

1. **Требования к результатам освоения дисциплины:**

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 1 Принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных	Этап 1 Уметь реализовывать политику безопасности баз данных	Этап 1 Навыки выявления организационных, программно- аппаратных и технических угроз безопасности база данных
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 2 Средства обеспечения безопасности данных	Этап 2 Применять средства обеспечения безопасности данных	Этап 2 Навыки проведения анализа защищенности автоматизированных систем
ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-8 -способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 2: основные методы технико-экономического обоснования проектных решений	Этап 2: проводить технико-экономическое обоснование проектных решений	Этап 2: навыки технико- экономического обоснования проектных решений
ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы	Этап 1основные составляющие политики безопасности	Этап 1: разрабатывать политик у безопасности	Этап 1: навыки разработки политики безопасности
ПК-11 – способностью разрабатывать политику информационно безопасности автоматизированной системы	Этап 2: принципы разработки политики безопасности	Этап 2: применять комплексный подход к обеспечению информацион-	Этап 2применения комплексного подхода к обеспечению информационной безопасности

		ной безопасности	
ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-12 – способностью участвовать в проектировании и системы управления информационно безопасностью автоматизированной системы	Этап 2: основные методы технико-экономического обоснования проектных решений	Этап 2: проводить технико-экономическое обоснование проектных решений	Этап 2: навыки технико- экономического обоснования проектных решений
ПК-13 -способностью участвовать в проектировании средств защиты информации автоматизированной системы	Этап 1: знать принцип ы построения криптографических алгоритмов	Этап 1: уметь выполнять настройки по обслуживанию криптосистем	Этап 1: выполнения настроек по обслуживанию криптосистем;
ПК-13 -способностью участвовать в проектировании средств защиты информации автоматизированной системы	Этап 2: знать криптографические стандарты и их использование в информационных системах	Этап 2: уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием криптосистем	Этап 2: осуществления мер противодействия нарушениям сетевой безопасности с использованием криптосистем
ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации	Этап 1: разрабатывать методик у контрольных проверок технических средств защиты информации	Этап 1: навыки применения контрольных проверок
ПК-14 -способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Этап 2: основные принципы работы технических средств защиты информации	Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 2: навыки оценки эффективности применении аппаратно-программных комплексов
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации	Этап 1: методику анализа информационной безопасности	Этап 1: разрабатывать методик у анализа информационной безопасности	Этап 1: разработки анализа информационной безопасности

в автоматизированной системе и выявлять каналы утеки информации			
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утеки информации	Этап 2: современные стандарты в области информационной безопасности	Этап 2: использовать стандарты в области информационной безопасности	Этап 2: использования стандартов в области информационной безопасности
ПК-19 – Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Этап 1 Общие методологические принципы построения комплексных систем обеспечения информационной безопасности;	Этап 1 Умения ми работы с нормативно-правовыми актами	Этап 1 Навыки участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
ПК-19– Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Этап 2 комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем;	Этап 2 Первичными навыкам и работы с основными средства ми обеспечения информационной безопасности	Этап 2 Навыки управления процессом реализации комплекса мер по обеспечению информационной безопасности
ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной без опасности автоматизированных систем	Этап 1: основные этапы оформления рабочей документации	Этап 1: разрабатывать основные рабочие документы	Этап 1: навыки разработки рабочих документов
ПК-21 -способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной без опасности автоматизированных систем	Этап 2: основные нормативные и методические документы	Этап 2: применять нормативные документы в рабочей документации	Этап 2: навыки применения нормативных документов
ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализа-	Этап 1основные составляющие политики безопасности	Этап 1: разрабатывать политику безопасности	Этап 1: навыки разработки политики безопасности

ции			
ПК-22 – способностью участвовать в формировании политик информационной безопасности организации и контролировать эффективность реализации	Этап 2: принцип ы разработки политики безопасности	Этап 2: применять комплексный подход к обеспечению информационной безопасности	Этап 2:применения комплексного подхода к обеспечению информационной безопасности
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	Этап 1: основные принципы администрирования	Этап 1: основные принципы администрирования	Этап 1: навыки администрирования подсистемы безопасности
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы)для защиты информации ограниченного доступа	Этап2:современные инструментальные средства администрирования	Этап 2: современные инструментальные средства администрирования инструментальные средства администрирования подсистемы безопасности	Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Этап 1: основные меры по выполнения обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 2: разработки мер поддержки обеспечения информационной безопасности

2. Содержание дисциплины:

Раздел 1 Введение в предмет

Тема 1 Основные элементы технологий открытых информационных систем

Тема 2 Совместимость, переносимость и способность взаимодействовать открытых систем. Основные модели открытых систем

Раздел 2 Интранет как открытая система

Тема 3 Уязвимость открытых систем на примере интранета. Базовые понятия. Основные угрозы. Уязвимость архитектуры клиент-сервер

Тема 4 Уязвимость открытых систем на примере интранета. Уязвимости системных утилит, команд, сервисов

Тема 5 Уязвимости современных технологий программирования. Ошибки в ПО

Раздел 3 Обеспечение информационной безопасности в открытых системах

Тема 6 Принципы создания защищенных средств связи объектов в открытых системах

Тема 7 Политика безопасности открытых систем

Тема 8 Управление безопасностью открытых систем

3. Общая трудоёмкость дисциплины: 5 ЗЕ