

Аннотация к рабочей программе дисциплины

Автор: Урбан В.А.

Наименование дисциплины: Б1.В.07 КОИБАС

Цель освоения дисциплины:

- подготовка к разработке системы управления информационной безопасностью автоматизированных систем, администрирование подсистем информационной безопасности автоматизированных систем.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ПК-6- способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Этап 1: общие методологические принципы построения комплексных систем обеспечения информационной безопасности;	Этап 1: проводить работы на автоматизированных системах специального назначения	Этап 1: основами инструментальным и средствами проектирования аппаратных и программных средств автоматизированных систем специального назначения
ПК-6- способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Этап 2: комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем	Этап 2: осуществлять установку, настройку и техническое сопровождение программного обеспечения	Этап 2: навыками оценки эффективности функционирования систем управления специального назначения
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап 1: рабочую техническую документацию	Этап 1: применять комплексные подходы к решению задач информационной безопасности	Этап 1: методами работы с нормативно-правовыми актами

<p>ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p>	<p>Этап 2: нормативные и методические документы</p>	<p>Этап 2: анализировать задачи информационной безопасности</p>	<p>Этап 2: навыками работы с нормативно-правовыми актами</p>
<p>ПК-13- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p>	<p>Этап 1: методы проектирования систем обеспечения информационной безопасности</p>	<p>Этап 1: использовать современные способы борьбы с несанкционированным доступом информации</p>	<p>Этап 1: средствами обнаружения, блокирования вторжений.</p>
<p>ПК-13- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p>	<p>Этап 2: средства проектирования систем обеспечения информационной безопасности</p>	<p>Этап 2: использовать методы копирования, изменения и сбора информации</p>	<p>Этап 2: современными средствами и системами сбора и защиты информации</p>
<p>ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и методическими документами</p>	<p>Этап 1: нормативные документы, регламентирующие работу ФСТЭК</p>	<p>Этап 1: проводить работы на автоматизированных системах специального назначения</p>	<p>Этап 1: основами инструментальным и средствами проектирования аппаратных и программных средств автоматизированных систем специального назначения</p>

ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами	Этап 2: нормативные документы, регламентирующие работу ФСБ	Этап 2: осуществлять установку, настройку и техническое сопровождение программного обеспечения	Этап 2: навыками оценки эффективности функционирования систем управления специального назначения
ПСК-4.3 – Способен планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Этап 1: методы оценки качества систем	Этап 1: планировать комплекс мероприятий по защите информации	Этап 1: первичными навыками работы с основными средствами обеспечения информационной безопасности.
ПСК-4.3 – Способен планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости	Этап 2: модели комплексной системы информационной безопасности	Этап 2: организовывать надежность защиты аппаратных и программных средств обработки информации	Этап 2: практическим опытом работы с основными средствами обеспечения информационной безопасности

аппаратных и программных средств обработки информации			
ПСК-4.4 – Способен участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Этап 1: программные и аппаратные средства АС	Этап 1: использовать современные способы борьбы с несанкционированным доступом информации	Этап 1: средствами обнаружения, блокирования вторжений.
ПСК-4.4 – Способен участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Этап 2: методику аттестации средств объектов информатизации	Этап 2: использовать методы копирования, изменения и сбора информации.	Этап 2: современными средствами и системами сбора и защиты информации

2. Содержание дисциплины:

Раздел 1 Угрозы ИБ.

Тема 1 Классификация угроз ИБ .

Тема 2 Анализ угроз ИБ.

Тема 3 Технические каналы утечки информации

Тема 4 Акустические каналы утечки информации.

Тема 5 ПЭМИН.

Тема 6 Закладные устройства.

Тема 7 Визуально-оптические каналы утечки информации.

Тема 8 Материально-вещественные каналы утечки информации.

Раздел 2 Постановка проблемы КОИБАС.

Тема 9 Методология построения КОИБАС.

Тема 10 Определение состава компонентов КСИБ.

Тема 11 Стадии и этапы проектирования КСИБ.

Тема 12 Формирование задач защиты информации.

Тема 13 Функциональные и обеспечивающие подсистемы КСИБ.

Тема 14 Правовые аспекты защиты информации.
Тема 15 Организационные мероприятия по защите информации.
Тема 16 Инженерно-технические мероприятия по ЗИ.
Раздел 3 Оценка качества КСИБ.
Тема 17 Политика информационной безопасности.
Тема 18 Модель нарушителя.
Тема 19 Классификация защищенности АС.
Тема 20 Оценка защищенности АС.
Тема 21 Аттестация объектов защиты.
Тема 22 Эксплуатационная документация КСИБ
Тема 23 Оценка технико-экономического уровня и эффективности КСИБ.
Тема 24 Управление деятельностью организации по КОИБАС.
Тема 25 Перспективы развития элементов КОИБАС.
Тема 26 Натурные испытания КС защиты.

3. Общая трудоёмкость дисциплины: 4 ЗЕ