Аннотация к рабочей программе дисциплины

Автор: Ю.В. Полищук

Наименование дисциплины: Б1.Б.1.32 Разработка и эксплуатация защищенных автоматизированных систем

Цель освоения дисциплины:

-теоретическая и практическая подготовка специалиста к построению автоматизированных систем в защищенном исполнении, которая включает освоение принципов системного подхода при создании сложных систем, современные тенденции программной инженерии,

-нормативно-методическое обеспечение создания автоматизированных систем, стандарт жизненного цикла автоматизированных систем, модели жизненного цикла автоматизированных систем, оценка процессов создания автоматизированных систем, методологии IDEF, проблематику комплексного обеспечения информационной безопасности автоматизированных систем, особенности синтеза комплексных систем информационной безопасности (КСИБ), методы и методики оценки КСИБ, аттестацию по требованиям безопасности, особенности эксплуатации КСИБ на объекте защиты, модели защиты информации и реализацию систем управления доступом.

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

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1 Цели, задачи, принципы и основные направления обеспечения криптографической информационной безопасности государства	Этап 1 Проводить анализ и давать оценку степени защищенности криптографической систем, осуществлять повышение уровня криптографической защиты с учетом развития всех видов обеспечений вычислительных систем	Этап 1 Профессиональной терминологией и методами теоретического обоснования в выборе оптимальной концепции криптографической безопасности

ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 2 Современные подходы к построению криптографических систем защиты информации	Этап 2 Применять отечественные и зарубежные стандарты криптографии в области компьютерной безопасности для проектирования , разработки и оценки защищенности компьютерных систем.	Этап 2 Владеть принципами оценки криптографической защищенности объектов информатизации и обеспечения требуемого уровня защиты
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 1: основные информационные технологии построения защищенных автоматизированных систем	Этап 1: Разрабатывать и использовать особенности информационных технологий	Этап 1: использования информационных технологий при организации системы защиты
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 2: Автоматизированные системы, применяемые при организации защиты информации	Этап 2: использовать особенности автоматизированных систем при организации системы защиты	Этап 2: навыки использования особенностей автоматизированных систем при организации системы защиты
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Этап 1: знать принципы построения криптографических алгоритмов	Этап 1: уметь выполнять настройки по обслуживанию криптосистем	Этап 1: выполнения настроек по обслуживанию криптосистем;
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	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-13- способностью участвовать в проектировании средств защиты информации автоматизирован ной системы	Этап 1: знать принципы 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 – 15- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Этап 1: методику проведения экспериментов	Этап 1: разрабатывать методику проведения экспериментов	Этап 1: разработки методики проведения экспериментов
ПК – 15- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Этап 2: методику обработки, оценки результатов экспериментов	Этап 2: разрабатывать методику обработки и оценки результатов эксперимента	Этап 2: разработки методики обработки и оценки результатов эксперимента

ПК-24– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизирован ной системы с учетом требований информационной безопасности	Знать Этап 1:общие методологически е принципы построения комплексных систем обеспечения информационной безопасности;	Уметь Этап 1: проводить работы на автоматизированных системах специального назначения	Владеть Этап 1: основами инструментальны ми средствами проектирования аппаратных и программных средств автоматизированных систем специального назначения
ПК-24– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизирован ной системы с учетом требований информационной безопасности	Этап 2: комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем	Этап 2: осуществлять инсталляцию, настройку и техническое сопровождение программного обеспечения	Этап 2: навыками оценки эффективности функционирования систем управления специального назначения
ПК-25 – способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизирован ной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Знать Этап 1: методы оценки качества систем	Уметь Этап 1: планировать комплекс мероприятий по защите информации	Владеть Этап 1: первичными навыками работы с основными средствами обеспечения информационной безопасности.

ПК-25 – способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизирован ной системы и восстановление их работоспособности при возникновении нештатных ситуаций	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
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. Проектирование и разработка автоматизированных информационных систем.

Тема 1 Введение

Тема 2 Понятие, виды и структура автоматизированных систем
Раздел 2 Работа с данными в автоматизированных информационных системах
Тема 3 Жизненный цикл АС
Тема 4 Порядок создания изделий ИТ, удовлетворяющих требованиям безопасности
Раздел 3 Разработка клиентского программного обеспечения
Тема 5 Технология доступа к базам данных ADO, BDE, ODBC, COM, CORBA
Тема 6 Клиенты удаленного доступа и построение запросов к СУБД
Раздел 4 Разработка клиентского программного обеспечения. Основные элементы клиентских программ
Тема 7 Объекты для работы с данными.
Тема 8 Администрирование и эксплуатация защищенных КС, эксплуатационная документация защищённых КС

3. Общая трудоёмкость дисциплины: 3 ЗЕ