

Аннотация рабочей программы дисциплины (модуля)
Б1.О.28 «Комплексное обеспечение защиты информации объекта информатизации»

Цель дисциплины

Изучение основ проектирования комплексной системы информационной безопасности (КСИБ), соотношения программных, аппаратных и организационных средств и методов в комплексной деятельности по защите информации (ЗИ) в автоматизированных системах (АС).

Задачи дисциплины

- освоение способов выделения информации в АС, подлежащей защите;
- изучение критериев защищённости АС, методологии построения современных КСИБ,
- технологий проектирования систем защиты информации;
- формирование комплексного подхода к обеспечению информационной безопасности АС.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знать основные методы принятия обоснованных экономических решений в профессиональной деятельности УК-9.2 Уметь принимать обоснованные экономические решения в различных областях жизнедеятельности УК-9.3 Иметь навыки принятия обоснованных экономических решений в различных областях жизнедеятельности
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа.
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем; ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;

		ОПК-10.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 - Знает номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных автоматизированных систем; ОПК-12.2 - Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-12.3 - Владеет навыками проектирования элементов защищенных автоматизированных систем и разработки необходимой технической документации в области проектирования защищенных автоматизированных систем с учетом действующих нормативных и методических документов.
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 - Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; ОПК-4.1.2 - Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; ОПК-4.1.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.

Содержание разделов дисциплины

Тема 1. Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)

Состав компонентов комплексной системы обеспечения информационной безопасности. Функциональные и обеспечивающие подсистемы, технология, управление. Законодательная, нормативно- методическая и научная базы разработки КСИБ. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС).

Тема 2. Методология формирования задач защиты; интеграция средств защиты в технологическую среду

Параллельная разработка АС и КСИБ. Системный подход к построению КСИБ. Архитектура защищенных АС. Соотношение программных, аппаратных и административных средств в комплексном обеспечении информационной безопасности АС. Разработка и содержание аварийного плана действий в случае нарушения ИБ АС.

Тема 3. Типовая структура КСИБ; методы проектирования и оценки качества КСИБ

Организация доступа к ресурсам АС. Система разграничения доступа к техническим средствам. Система разграничения доступа к программам и данным. Средства блокировки неправомерных действий субъектов. Задача интеграции средств защиты информации в

технологическую среду АС. Требования к составу проектной и эксплуатационной документации. Порядок подготовки и проведения аттестации АС. Сертификация программного обеспечения.

Тема 4. Этапы проектирования КСИБ и требования к ним

Предпроектное обследование: инвентаризация ресурсов. Предпроектное обследование: модели угроз и нарушителя. Предпроектное обследование: анализ рисков. Техническое задание. Техническое и рабочее проектирование. Испытания и внедрение в эксплуатацию, сопровождение. Оценка эффективности. Особенности проектирования на современном уровне и синтез КСИБ. Автоматизация процесса анализа и управления рисками. Моделирование процедуры.

Тема 5. Структура политики информационной безопасности организации (ПИБ)

Методики формирования ПИБ верхнего уровня (цели, концепции, доктрины). Методики формирования ПИБ среднего уровня (стандарты). Способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции). Типовой перечень задач службы информационной безопасности. Организационно-технические и режимные меры.