Аннотация к рабочей программе дисциплины

Автор: Фот Ю.Д, доцент

Наименование дисциплины: Б1.В.10 Информационная безопасность значимых объектов критической информационной инфраструктуры (кии)

Цель освоения дисциплины: заключается в изучении нормативно правовых актов, методических документов и национальных стандартов в области обеспечения безопасности значимых объектов КИИ, основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, общие требования по обеспечению безопасности значимых объектов КИИ, общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования, научиться определять категории значимости объектов КИИ, а также в определении структуры системы безопасности значимого объекта КИИ.

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	*Знать:* Нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ и АСУТПиП; основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации; основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования; процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости

		присвоения ему одной из таких категорий *Уметь:* Определять структуру системы безопасности значимого объекта КИИ; осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ *Владеть:* Навыками разработки организационно-распорядительныхдокументов по безопасности значимых объектов КИИ
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	*Знать:* Общие требования по обеспечению безопасности значимых объектов КИИ; общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования; требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ *Уметь:* Определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации; определять требования к

		обеспечению безопасности значимого объекта КИИ *Владеть:* Навыками проведения работ по контролю состояния безопасности объектов КИИ
ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базамиданных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* Процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ *Уметь:* Выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации *Владеть:* Навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ
	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* Общие требования по обеспечению безопасности значимых объектов КИИ; общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования; требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ; *Уметь:* Обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта

		КИИ *Владеть:* Навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ
ПК-6 Способен проводитьанализ рисков информационной безопасности автоматизированнойсистемы	ПК-6.1 Проводит оценкурисков информационной безопасности на основе существующих методик	*Знать:* Основные принципы выявления наличия критических процессов у субъекта КИИ; основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и(или) осуществляют управление, контроль или мониторинг критических процессов; процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ *Уметь:* Выявлять возможные уязвимости, приводящих к возникновению рисков безопасности информации *Владеть:* Навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами

2. Содержание дисциплины:

Тема1. Введение в безопасность объектовкритической информационной инфраструктуры. Основные термины иопределения. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. Правовые основы обеспечения безопасности КИИ Российской Федерации. Федеральные законы. Указы Президента РФ.Постановления Правительства РФ.Приказы ФСТЭК России и ФСБ России.

Тема 2. Объекты и субъекты КИИ. Правила категорирования объектов КИИ. Общий порядок работ. Критерии значимости объектов КИИ.Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ. Создание комиссии по категорированию. Формирование перечня критических процессов.

Формирование перечняобъектов критической информационной инфраструктуры, подлежащих категорированию. Категорирование объектов критической информационной инфраструктуры. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозыбезопасности информации объекта КИИ. Построение модели угроз и нарушителей объектовКИИ. Процедурывыявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ. Оценка масштаба последствийи соотнесение со значениями показателей категорий. Определение категории значимостиобъекта КИИ. Оформление и передачав ФСТЭК России результатов категорирования. Внесение изменений в результаты категорирования. Подготовка отчетныхдокументов и контроль результатов категорированияобъектов КИИ.

Тема 3. Требования по обеспечению безопасности значимых объектов КИИ РФ. Требования ксредствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак иреагирования на компьютерные инциденты. Требованияк параметрам настройкипрограммных и программно-аппаратных средств, включая средствазащиты информации, обеспечивающие реализацию, мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации Система безопасности значимого объекта КИИ. Порядок,технические условияустановки и эксплуатации средств,предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Стадии (этапы) работ по созданию систем безопасности объекта КИИ. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования. Разработка организационно- распорядительных документов по безопасности значимых объектов КИИ

Тема 4. Правила осуществления госконтроля в областиобеспечения безопасности значимых объектов КИИ РФ. Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК. Порядок ведения реестра значимых объектов КИИ РФ. Итоги проведения госконтроля в области обеспечения безопасности значимыхобъектов КИИ РФ. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственным и организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.

Тема 5. Перечень информации, представляемой в ГосСОПКА и порядок представления информации в ГосСОПКА. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).

Тема 6. Обследование АСУ ТП. Разработка требований по обеспечению безопасности информации в АСУ ТП.Разработка концепции ОБИ в АСУ ТП. Разработка Технического

задания на создание системызащиты АСУ ТП. Проектирование системы защиты АСУТП. Внедрение системызащиты АСУ ТП.Разработка комплектаорганизационно-распорядительной документации, регламентирующей процессы защиты АСУТП.

Тема 7. Аудиткритической информационной инфраструктуры. Особенности проведения аудиткритической информационной инфраструктуры. Определение аудита информационной безопасности. Цели изадачи аудита. Этапы проведения аудита. Схема проведения аудита. Общие подходык проведению аудита. Классификация аудита. Тестирование как одиниз основных типов аудита критической информационной инфраструктуры. Тестирование: определение, требования, классификация. Тестирование на основе моделей. Тестирование специальными средствами и способами информационных воздействий. Особенности тестирования критической инфраструктуры информационными воздействиями втехнической и впсихологических сферах. Тестирование критической инфраструктурыспециальными информационно-техническими воздействиями. Общая классификация информационно- технических воздействий. Оборонительные информационно-технические воздействия. Обеспечивающие информационно- технические воздействия. Атакующие информационно технические воздействия. Классификация основных средств информационно- технических воздействий.

Тема 8. Модели правового регулирования в сфере обеспечения безопасности КИИ. Невластные субъекты обеспечения безопасности КИИ, их правовой статус.Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами. Сравнительно- правовой анализпредлагаемых экономических моделей распределения издержек по обеспечению безопасности КИИ.

3. Общая трудоемкость дисциплины: 4 ЗЕ